

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2001-209583
(P2001-209583A)

(43) 公開日 平成13年8月3日(2001.8.3)

(51) Int.Cl. ⁷	識別記号	F I	マーク-1 ⁸ (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
	12/00	5 3 7	3 2 0 F 5 B 0 8 2
G 0 9 C 1/00	6 4 0	12/00	5 3 7 H 5 D 0 4 4
G 1 1 B 20/10		G 0 9 C 1/00	6 4 0 Z 5 J 1 0 4
		G 1 1 B 20/10	H 9 A 0 0 1

(21)出願番号 特願2000-16469(P2000-16469)

(71) 出願人 000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号

(71) 出願人 395015319
株式会社ソニー・コンピュータエンタテイメント
東京都港区赤坂7-1-1

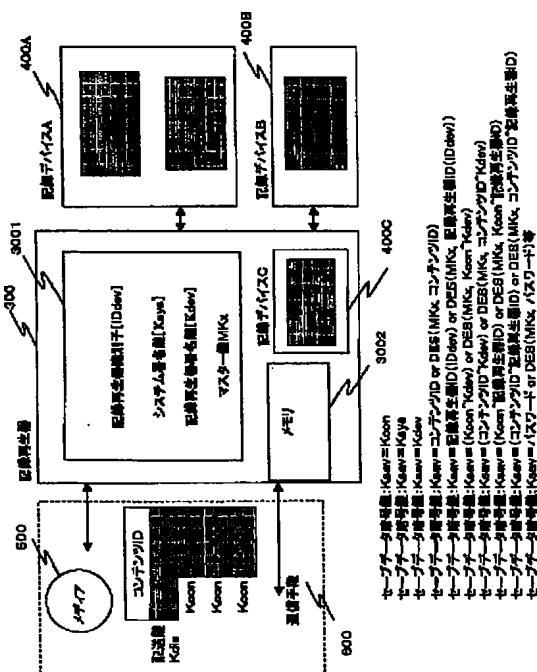
(72) 発明者 浅野 智之
東京都品川区北品川6丁目7番35号 ソニー
株式会社内

(74) 代理人 100101801
弁理士 山田 英治 (外2名)

最終頁に統ぐ

(54) [発明の名称] データ記録再生器およびデータ処理方法、並びにプログラム提供媒体

(57) 【要約】 【課題】 セーブデータのセキュリティを確保可能としたデータ記録再生器およびセーブデータ処理方法を提供する。【解決手段】 プログラムのみに固有な暗号鍵、例えばコンテンツ鍵、またはコンテンツ鍵に基づいてセーブデータ暗号化鍵を生成してセーブデータを暗号化して記録デバイスに格納し、再生時はプログラム固有のセーブデータ復号化鍵によって復号処理を実行する。さらに、記録再生器固有の鍵、あるいはユーザパスワードを用いてセーブデータ暗号鍵、復号鍵を生成してセーブデータの暗号化、復号化を実行してセーブデータの格納、再生を実行する等、各種の制限情報に基づくセーブデータ暗号鍵の生成を可能とした。



入力または設定である場合、前記記録再生器に格納されたシス前記データ記録再生器に格納されたシステム共通の暗号またはシステム共通の暗号鍵に基づいて生成される共通セーブデータ暗号鍵によってセーブデータの暗号化処理または復号化処理を実行する構成であることを特徴とする請求項1に記載のデータ記録再生器。【請求項7】前記システム署名鍵K_{s y s}であることを特徴とする請求項6に記載のデータ記録再生器。【請求項8】プログラムコンテンツを再生実行可能なデータ記録再生器におけるセーブデータ処理方法において、入力手段からの入力使用制限情報に従って、記録デバイスに対して格納するセーブデータの暗号化処理態様を決定する暗号化処理態様決定ステップと、前記暗号化処理態様決定ステップと、前記暗号化処理態様決定ステップにデータ記録再生器におけるセーブデータの暗号化処理を実行することを特徴とするセーブデータ処理方法。【請求項9】前記セーブデータファイルに設定された設定使用制限情報に従って、記録デバイスからの再生セーブデータの復号化処理態様を決定するプログラム制限であり、プログラム制限ありの場合は、前記復号化処理態様決定ステップと、前記復号化処理態様決定ステップと、前記復号化処理態様決定ステップにおいて選択された復号化鍵を用いてセーブデータの復号化処理を実行することを特徴とするセーブデータ処理方法。【請求項10】前記セーブデータ処理方の同一性を条件としてセーブデータの利用を可能とする記録再生器制限であり、記録再生器制限ありの場合は、前記記録再生器に固有の暗号鍵または固有の情報の少なくともいずれかに基づいて生成される記録再生器固有セーブデータ暗号鍵を暗号化処理に適用する暗号化鍵として選択し、記録再生器制限なしの場合は、

鍵、またはシステム共通の暗号鍵に基づいて生成される共通セーブデータ暗号鍵を暗号化処理に適用する暗号化鍵として選択することを特徴とする請求項8に記載のセーブデータ暗号化処理方法。【請求項11】前記セーブデータ処理方法に条件としてセーブデータの利用を可能とするユーザ制限であり、ユーザ制限ありの場合は、前記暗号化鍵選択ステップに生成されるユーザ固有セーブデータ暗号鍵を暗号化処理に適用する暗号化鍵として選択し、記録再生器制限なしの場合は、鍵、またはシステム共通の暗号鍵に基づいて生成される共通セーブデータ暗号鍵を暗号化処理に適用する暗号化鍵として選択することを特徴とする請求項8に記載のセーブデータ処理方法。【請求項12】プログラムコンテンツを再生する記憶手段または記録デバイスに格納されたデータ管理プログラムの同一性を条件としてセーブデータの利用を可能とするプログラム制限であり、プログラム制限ありの場合は、前記復号化処理態様決定ステップと、前記復号化処理態様決定ステップと、前記復号化処理態様決定ステップにおいて選択された復号化鍵を用いてセーブデータの復号化処理を実行することを特徴とするセーブデータ処理方法。【請求項13】前記セーブデータの同一性を条件としてセーブデータの利用を可能とするプログラム制限であり、プログラム制限ありの場合は、前記復号化処理態様決定ステップと、前記復号化処理態様決定ステップにおいて選択された復号化鍵を用いてセーブデータの復号化処理を実行することを特徴とするセーブデータ処理方法。【請求項14】前記セーブデータ復号化鍵を復号化処理に適用する復号化鍵として選択し、プログラム制限なしの場合は、前記データ記録再生器固有セーブデータ復号化鍵を復号化処理に適用する復号化鍵として選択し、プログラム制限なしの場合は、前記データ記録再生器固有セーブデータ復号化鍵を復号化処理に適用する復号化鍵として選択することを特徴とする請求項12に記載のセーブデータ処理方法。

【請求項14】前記セーブデータ処理方法において、前の同一性を条件としてセーブデータの利用を可能とする記録再生器制限であり、記録再生器制限ありの場合は、記録再生器に固有の暗号鍵または固有の情報の少なくともいずれかに基づいて生成される記録再生器固有セーブデータ復号化鍵を復号化処理に適用する復号化鍵として選択し、記録再生器制限なしの場合は、前記データ記録再生鍵、またはシステム共通の暗号鍵に基づいて生成される共通セーブデータ復号化鍵を復号化処理に適用する復号化鍵として選択することを特徴とする請求項12に記載のセーブデータ処理方法。【請求項15】前記セーブデータ条件としてセーブデータの利用を可能とするユーザ制限

であり、ユーザ制限ありの場合は、前記復号化鍵選択が生成されるユーザ固有セーブデータ復号化鍵を復号化処理に適用する復号化鍵として選択し、記録再生器制限な鍵、またはシステム共通の暗号鍵に基づいて生成される共通セーブデータ復号化鍵を復号化処理に適用する復号化鍵として選択することを特徴とする請求項1-2に記載のセーブデータ処理方法。【請求項1-6】プログラムコードデータ記録再生器におけるセーブデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、入力手段からの入力使用制限スに対し格納するセーブデータの暗号化処理態様を決定する暗号化処理態様決定ステップと、前記暗号化処理化処理態様に応じて暗号化処理に適用する暗号化鍵を選択する暗号化鍵選択ステップと、前記暗号化鍵選択ステップを用いてセーブデータの暗号化処理を実行するステップと、を有することを特徴とするプログラム提供媒体。【データ記録再生器におけるセーブデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラム】

ラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、記憶手段または記録デバイスに格納され、復元に設定された設定使用制限情報に従って、記録デバイスの暗号化デバイスから再生するセーブデータの復号化処理態様を決定する復号化処理態様決定ステップと、前記復号化処理態様決定ステップに応じて復号化処理に適用する復号化鍵を選択する復号化鍵選択ステップと、前記復号化鍵選択ステップにおいて用いてセーブデータの復号化処理を実行するステップと、を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】 【0001】 【発明の属する技術分野】 本発明は、データ記録再生器、記録デバイス、記録媒体、データ記録再生方法、データ記録方法、データ記録装置、データ記録再生装置、データ記録再生方法並びにプログラム提供媒体の暗号化方法、データ記録再生装置の構成要素、データ記録再生装置の構成要素並びにデータ記録再生装置の構成要素の組合せに関するものである。【0002】 本発明は、DVD、CD等の記録媒体、CATV、インターネット、衛星通信等の有線、無線各通信手段等の経路で入手可能な音声、画像、ゲーム、プログラム等の各種コンテンツを、ユーザの所有する記録再生器において再生し、専用の記録デバイス、例えばメモリカード、ハードディスク、CD-R等に格納するとともに、実行途中のゲームデータ等のセーブデータを、十分なセキュリティおよび様々な使用制限を付して記録デバイスに格納、または再生処理することを可能としたデータ記録再生器およびセーブデータ処理方法に関するものである。【0003】 【従来の技術】 昨今、ゲームプログラム、音楽データ、画像データ、文書作成プログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはDVD、CD等の流通可能な記憶媒体を介して流通している。これらの流通コンテンツは、ユーザの所有するPC（Personal Computer）、ゲーム機器等の記録再生機器に付属する記録デバイス、例えばメモリカード、ハードディスク等に格納することが可能であり、一旦格納された後は、格納媒体からの再生により利用可能となる。【0004】 従来のビデオゲーム機器、PC等の情報機器において使用されるメモリカード装置の主な構成要素

は、動作制御のための制御手段と、制御手段に接続され情報機器本体に設けられたスロットに接続するためのコネクタと、制御手段に接続されデータを記憶するための不揮発性メモリ等である。メモリカードに備えられた不揮発性メモリはE E P R O M、フラッシュメモリ等によって構成される。【0005】このようなメモリカードに記憶する、あるいはプログラム等の様々なコンテンツは、再生機器として利用されるゲーム機器、P C等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により不揮発性メモリから呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。【0006】ゲームプログラム等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。【0007】ユーザに対する利用制手法が、配布コンテンツの暗号化処理である。すなわち、例えばインターネット等を介して暗号化された音声データ、画像データ、ゲームプログラム等の各種コンテンツを配布するとともに、正規ユーザであると確認された者に対してのみ、配布された暗号化コンテンツを復号する手段、すなわち復号鍵を付与する構成である。【0008】暗号化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。【0009】暗号化鍵・復号化方法の態様には様々な種類あるが、その1つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にD E S（データ暗号標準：Data encryption standard）がある。【0010】上述の暗号化処理、復号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成する

ものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めるることは実質上不可能となる。このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。【0011】また、暗号化するときに使用する暗号化鍵による処理と、復号するときに使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が発行した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を発行した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものにはR S A（Rivest-Shamir-Adleman）暗号がある。【0012】さらに、記録再生器にはアクセス可録デバイスが複数存在するのが一般的である。例えば、D V D、C D、メモリカード、ハードディスク等である。ユーザはこれらの複数の機器から例えばゲームプログラムを選択して実行する場合、各記録デバイス内のコンテンツデータの内容を各デバイスを逐次アクセスして確認し、再生しようとするコンテンツを格納した機器を特定し、その後、プログラムを実行することが必要となり、プログラム起動開始までに時間を要することになる。コンテンツを利用するデータ処理装置構成について図1を用いて簡単に説明する。【0013】図1は、P C（パソコン）、ゲーム機器等の再生手段10において、D V D、C D 3 0、インターネット40等のデータ提供手段から取得したプログラム、音声データ、映像データ等（コンテンツ（Content））を再生するとともに、D V D、C D 3 0、インターネット40等から取得したデータをフロッピーディスク、メモリカード、ハードディスク等の記憶手段20に記憶可能とした構成例を示すものである。【0014】プログラム、音声データ、映像データ等の復コンテンツは、暗号化処理がなされ、再生手段10を有するユーザに提供される。正規ユーザは、暗号化データとともに、その暗号化、復号化鍵である鍵データを取得する。【0015】再生手段10はC P U 1 2を有し、入力データの再生処理を再生処理部14で実行する。再生処理部14は、暗号化データの復号処理を実行して、提供されたプログラムの再生、音声データ、画像データ等コンテンツ再生を行なう。

【0016】正規ユーザは、提供されたプログラムを、再度使用するために記憶手段20にプログラム/データ等、コンテンツの保存処理を行なう。再生手段10には、このコンテンツ保存処理を実行するための保存処理部13を有する。保存処理部13は、記憶手段20に記憶されたデータの不正使用を防止するため、データに暗号化処理を施して保存処理を実行する。【0017】コンテンツ暗号用鍵を用いる。保存処理部13は、コンテンツ暗号用鍵を用いて、コンテンツを暗号化し、それをFD(フロッピーディスク)、メモリカード、ハードディスク等の記憶手段20の記憶部21に記憶する。【0018】ツを取り出して再生する場合には、記憶手段20から、暗号化データを取り出して、再生手段10の再生処理部14において、コンテンツ復号用の鍵、すなわち復号化鍵を用いて復号処理を実行して暗号化データから復号データを取得して再生する。【0019】また、再生手段10にコンテンツがゲームプログラム等である場合、例えばゲームプログラムを途中で中断して、所定時間後、新たに再開しようとする場合には、中断時点のゲーム状態等をセーブ、すなわち記録デバイスに格納し、これを再開時に読み出してゲームを続行する、いわゆるセーブデータ記録再生処理が従来から行われている。【0020】【発明が解説】ソコン等の記録再生器におけるセーブデータ保存構成は、例えば記録再生器に内蔵、あるいは外付け可能なメモリカード、フローピーディスク、ゲームカートリッジ、あるいはハードディスク等の記憶媒体にセーブデータを保存する構成を持つが、特に、そのセーブデータに対するセキュリティ確保構成を有しておらず、例えばゲームアプリケーションプログラムに共通の仕様でデータのセーブ処理が行われる構成となっている。【0021】用いてセーブされたセーブデータが別のゲームプログラムによって使用されたり、書換えられたり、上書きされたりする事態が発生してしまい、セーブデータのセキュリティはほとんど考慮されていなかった。【0022】本セーブデータのセキュリティ確保を実現可能とした構成を提供する。例えばあるゲームプログラムのセーブデータは、そのゲームプログラムのみに固有な情報に基づいて暗号化して記録デバイスに格納する。あるいは、記録再生器固有の情報に基づいて暗号化して記録デバイスに格納する。これらの手法により、セーブデータの利用を特定の機器、特定のプログラムのみに制限することができる。本発明は、このような手法を適用することによりセーブデータのセキュリティを確保可能としたデータ記

録再生器およびセーブデータ処理方法を提供する。【0023】プログラムコンテンツを再生実行可能なデータ記録再生器において、前記プログラムコンテンツに関するセーブデータを記録する記録デバイスと、前記記録デバイスに対する格納セーブデータの暗号化処理および前記記録デバイスから再生する再生セーブデータの復号化処理を実行する暗号処理部と、セーブデータの使用制限情報を入力する入力手段と、セーブデータの暗号化処理方法または復号化処理方法を決定する制御部とを有し、前記制御部は、前記入力手段からの入力使用制限情報に従って、前記記録デバイスに対して格納するセーブデータの暗号化処理方法を決定するとともに、前記制御部がアクセス可能な記憶部または記録デバイスに格納したデータ管理ファイルに設定されたセーブデータ使用制限情報に従って、前記記録デバイスから再生するセーブデータの復号化処理方法を決定する構成を有し、前記暗号処理部は、前記制御部の決定した暗号化処理方法または復号化処理方法に応じて異なる暗号鍵を用いてセーブデータの暗号化処理または復号化処理を実行する構成を有することを特徴とするデータ記録再生器にある。【0024】さらに、本発明の施設において、前記セーブデータの使用制限情報は、コンテンツプログラムの同一性を条件としてセーブデータの利用を可能とするプログラム制限であり、前記データ管理ファイルは、コンテンツプログラムの識別子に対応させてプログラム制限情報を格納したテーブルとして構成され、前記暗号処理部は、前記入力手段からの入力使用制限情報、または前記データ管理ファイルの設定使用制限情報がプログラム制限ありの入力または設定である場合、前記コンテンツプログラムに固有の暗号鍵、またはコンテンツプログラムに固有の暗号鍵または固有の情報の少なくともいずれかに基づいて生成されるプログラム固有セーブデータ暗号鍵によってセーブデータの暗号化処理または復号化処理を実行し、前記入力手段から本発明の入力使用制限情報、または前記データ管理ファイルの設定使用制限情報がプログラム制限なしの入力または設定である場合、前記データ記録再生器に格納されたシステム共通の暗号鍵、またはシステム共通の暗号鍵に基づいて生成される共通セーブデータ暗号鍵によってセーブデータの暗号化処理または復号化処理を実行する構成であることを特徴とする。【0025】さらに、本発明のデータ記録再生器において、前記コンテンツプログラムに固有の暗号鍵は、前記コンテンツプログラムを含むコンテンツデータのヘッダ部に格納されたコンテンツ鍵K_{con}であり、前記システム共通の暗号鍵は、複数の異なるデータ記録再生器に共通に格納されたシステム署名鍵K_{sys}であることを特徴とする。

【0026】さらに、本発明のデータ記録再生器の一実施態様において、前記セーブデータの使用制限情報は、データ記録再生器の同一性を条件としてセーブデータの利用を可能とする記録再生器制限であり、前記データ管理ファイルは、コンテンツプログラムの識別子に対応させて記録再生器制限情報を格納したテーブルとして構成され、前記暗号処理部は、前記入力手段からの入力使用制限情報、または前記データ管理ファイルの設定使用制限情報が記録再生器制限ありの入力または設定である場合、前記データ記録再生器に固有の暗号鍵、またはデータ記録再生器に固有の暗号鍵または固有の情報の少なくともいずれかに基づいて生成される記録再生器固有セーブデータ暗号鍵によってセーブデータの暗号化処理または復号化処理を実行し、前記入力手段からの入力使用制限情報、または前記データ管理ファイルの設定使用制限情報がプログラム制限なしの入力または設定である場合、前記データ記録再生器に格納されたシステム共通の暗号鍵、またはシステム共通の暗号鍵に基づいて生成される共通セーブデータ暗号鍵によってセーブデータの暗号化処理または復号化処理を実行する構成であることを特徴とする。【0027】さらに、本発明のデータ記録再生器施態様において、前記データ記録再生器に固有の暗号鍵は、前記データ記録再生器に格納された該データ記録再生器固有の署名鍵K_{d e v}であり、前記システム共通の暗号鍵は、複数のデータ記録再生器に共通に格納されたシステム署名鍵K_{s y s}であることを特徴とする。【0028】さらに、本発明のデータ記録再生器施態様において、前記セーブデータの使用制限情報は、ユーザの同一性を条件としてセーブデータの利用を可能とするユーザ制限であり、前記データ管理ファイルは、コンテンツプログラムの識別子に対応させてユーザ制限情報を格納したテーブルとして構成され、前記暗号処理部は、前記入力手段からの入力使用制限情報、または前記データ管理ファイルの設定使用制限情報がユーザ制限ありの入力または設定である場合、前記入力手段から入力されるパスワード、または該パスワードに基づいて生成されるユーザ固有セーブデータ暗号鍵によってセーブデータの暗号化処理または復号化処理を実行し、前記入力手段からの入力使用制限情報、または前記データ管理ファイルの設定使用制限情報がユーザ制限なしの入力または設定である場合、前記記録再生器に格納されたシステム共通の暗号鍵、またはシステム共通の暗号鍵に基づいて生成される共通セーブデータ暗号鍵によってセーブデータの暗号化処理または復号化処理を実行する構成であることを特徴とする。【0029】さらに、本発明のデータ記録再生器施態様において、前記システム共通の暗号鍵は、複数の記録再生器に共通に格納されたシステム署名鍵K_{s y s}であることを特徴とする。

【0030】さらに、本発明の第2の側面は、プログラムコンテンツを再生実行可能なデータ記録再生器におけるセーブデータ処理方法において、入力手段からの入力使用制限情報に従って、記録デバイスに対して格納するセーブデータの暗号化処理態様を決定する暗号化処理態様決定ステップと、前記暗号化処理態様決定ステップにおいて決定した暗号化処理態様に応じて暗号化処理に適用する暗号化鍵を選択する暗号化鍵選択ステップと、前記暗号化鍵選択ステップにおいて選択された暗号化鍵を用いてセーブデータの暗号化処理を実行することを特徴とするセーブデータ処理方法である。【0031】さらに、本発明一実施態様において、前記セーブデータの使用制限情報は、コンテンツプログラムの同一性を条件としてセーブデータの利用を可能とするプログラム制限であり、プログラム制限ありの場合は、前記暗号化鍵選択ステップにおいて、前記コンテンツプログラムに固有の暗号鍵、またはコンテンツプログラムに固有の暗号鍵または固有の情報の少なくともいずれかに基づいて生成されるプログラム固有セーブデータ暗号鍵を暗号化処理に適用する暗号化鍵として選択し、プログラム制限なしの場合は、前記データ記録再生器に格納されたシステム共通の暗号鍵、またはシステム共通の暗号鍵に基づいて生成される共通セーブデータ暗号鍵を暗号化処理に適用する暗号化鍵として選択することを特徴とする。【0032】さらに、本発明一実施態様において、前記セーブデータ処理方法において、前記セーブデータの使用制限情報は、データ記録再生器の同一性を条件としてセーブデータの利用を可能とする記録再生器制限であり、記録再生器制限ありの場合は、前記暗号化鍵選択ステップにおいて、前記データ記録再生器に固有の暗号鍵、またはデータ記録再生器に固有の暗号鍵または固有の情報の少なくともいずれかに基づいて生成される記録再生器固有セーブデータ暗号鍵を暗号化処理に適用する暗号化鍵として選択し、記録再生器制限なしの場合は、前記データ記録再生器に格納されたシステム共通の暗号鍵、またはシステム共通の暗号鍵に基づいて生成される共通セーブデータ暗号鍵を暗号化処理に適用する暗号化鍵として選択することを特徴とする。【0033】さらに、本発明のセーブデータ処理方法の一実施態様において、前記セーブデータ処理方法において、前記セーブデータの使用制限情報は、ユーザの同一性を条件としてセーブデータの利用を可能とするユーザ制限であり、ユーザ制限ありの場合は、前記暗号化鍵選択ステップにおいて、ユーザ入力パスワード、または該パスワードに基づいて生成されるユーザ固有セーブデータ暗号鍵を暗号化処理に適用する暗号化鍵として選択し、記録再生器制限なしの場合は、前記データ記録再生器に格納されたシステム共通の暗号鍵、またはシステム

共通の暗号鍵に基づいて生成される共通セーブデータ暗号鍵を暗号化処理に適用する暗号化鍵として選択することを特徴とする。【0034】さらに、本発明の第3の側面は、ムコンテンツを再生実行可能なデータ記録再生器におけるセーブデータ処理方法において、記憶手段または記録デバイスに格納されたデータ管理ファイルに設定された設定使用制限情報に従って、記録デバイスからの再生セーブデータの復号化処理態様を決定する復号化処理態様決定ステップと、前記復号化処理態様決定ステップにおいて決定した復号化処理態様に応じて復号化鍵を選択する復号化鍵選択ステップと、前記復号化鍵選択ステップにおいて選択された復号化鍵を用いてセーブデータの復号化処理を実行することを特徴とするセーブデータ処理方法にある。【0035】さらに、本発明のセーブデータ処理の一実施態様において、前記セーブデータの使用制限情報は、コンテンツプログラムの同一性を条件としてセーブデータの利用を可能とするプログラム制限であり、プログラム制限ありの場合は、前記復号化鍵選択ステップにおいて、前記コンテンツプログラムに固有の暗号鍵、またはコンテンツプログラムに固有の暗号鍵または固有の情報の少なくともいすれかに基づいて生成されるプログラム固有セーブデータ復号化鍵を復号化処理に適用する復号化鍵として選択し、プログラム制限なしの場合は、前記データ記録再生器に格納されたシステム共通の暗号鍵、またはシステム共通の暗号鍵に基づいて生成される共通セーブデータ復号化鍵を復号化処理に適用する復号化鍵として選択することを特徴とする。【0036】さらに、一実施態様において、前記セーブデータの使用制限情報は、データ記録再生器の同一性を条件としてセーブデータの利用を可能とする記録再生器制限であり、記録再生器制限ありの場合は、前記復号化鍵選択ステップにおいて、前記データ記録再生器に固有の暗号鍵、またはデータ記録再生器に固有の暗号鍵または固有の情報の少なくともいすれかに基づいて生成される記録再生器固有セーブデータ復号化鍵を復号化処理に適用する復号化鍵として選択し、記録再生器制限なしの場合は、前記データ記録再生器に格納されたシステム共通の暗号鍵、またはシステム共通の暗号鍵に基づいて生成される共通セーブデータ復号化鍵を復号化処理に適用する復号化鍵として選択することを特徴とする。【0037】さらに、本発明の一実施態様において、前記セーブデータの使用制限情報は、ユーザの同一性を条件としてセーブデータの利用を可能とするユーザ制限であり、ユーザ制限ありの場合は、前記復号化鍵選択ステップにおいて、ユーザ入力パスワード、または該パスワードに基づいて生成されるユーザ固有セーブデータ復号化鍵を復号化処理に適用する

復号化鍵として選択し、記録再生器制限なしの場合は、前記データ記録再生器に格納されたシステム共通の暗号鍵、またはシステム共通の暗号鍵に基づいて生成される共通セーブデータ復号化鍵を復号化処理に適用する復号化鍵として選択することを特徴とする。【0038】さらに、本発明のムコンテンツを再生実行可能なデータ記録再生器におけるセーブデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、入力手段からの入力使用制限情報に従って、記録デバイスに対して格納するセーブデータの暗号化処理態様を決定する暗号化処理態様決定ステップと、前記暗号化処理態様決定ステップにおいて決定した暗号化処理態様に応じて暗号化処理に適用する暗号化鍵を選択する暗号化鍵選択ステップと、前記暗号化鍵選択ステップにおいて選択された暗号化鍵を用いてセーブデータの暗号化処理を実行するステップと、を有することを特徴とするプログラム提供媒体にある。【0039】さらに、本発明の第5の側面は、ムコンテンツを再生実行可能なデータ記録再生器におけるセーブデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、記憶手段または記録デバイスに格納されたデータ管理ファイルに設定された設定使用制限情報に従って、記録デバイスから再生するセーブデータの復号化処理態様を決定する復号化処理態様決定ステップと、前記復号化処理態様決定ステップにおいて決定した復号化処理態様に応じて復号化処理に適用する復号化鍵を選択する復号化鍵選択ステップと、前記復号化鍵選択ステップにおいて選択された復号化鍵を用いてセーブデータの復号化処理を実行するステップと、を有することを特徴とするプログラム提供媒体にある。【0040】本発明に係るプログラムuebaば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。【0041】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムとの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【0042】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。【0043】する。説明の手順は、以下の項目に従って行なう。(1) 理 (6-1) 相互認証処理の概要 (6-2) 相互認証時理 (8) 記録デバイス格納情報の記録再生器での再生処理 (10) オーディオマットに対応するダウンロードおよび再生処理 (11) C V 生成処理態様 (12) マスタ鍵に基づく暗号処理 (13) 先順位に基づくプログラム起動処理 (15) コンテンツ格納、再生処理 (17) 不正機器の排除 (リボケーション) (18) 成プロック図を示す。本発明のデータ処理装置は、記録再生器 300 と記録デバイス 400 を主要構成要素とする。【0045】記録再生器 300 は、例えばパソコン (PC : Personal Computer)、あるいはゲーム機器等によって構成される。記録再生器 300 は、図 2 に示すように、記録再生器 300 における暗号処理時の記録デバイス 400 との通信制御を含む統括的制御を実行する制御部 301、暗号処理全般を司る記録再生器暗号処理部 302、記録再生器に接続される記録デバイス 400 と認証処理を実行しデータの読み書きを行う記録デバイスコントローラ 303、DVDなどのメディア 500 から少なくともデータの読み出しを行う読み取り部 304、外部とデータの送受信を行う通信部 305 を有する。【0046】記録再生器 300 は、制御

るが、記録再生器300において実行される相互認証処理、チェック値照合処理、暗号化、復号化処理等、各種処理において必要となる鍵データ、あるいは識別データ等を格納する。【0053】暗号/復号化部308は、内部メモリ307に格納された鍵データ等を使用して、外部から入力されるコンテンツデータを記録デバイス400にダウンロード処理する際、あるいは記録デバイス400に格納されたコンテンツデータを記録デバイス400から再生、実行する際の認証処理、暗号化処理、復号化処理、さらに所定のチェック値や電子署名の生成・検証、データの検証、乱数の発生などの処理を実行する。【0054】この部メモリ307は、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しが容易な構造にしておく必要がある。従って、暗号処理部302は、外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または/かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する耐タンパクメモリとして構成される。この構成については、後段で詳細に説明する。【0055】記録再生器300は、他の機能に、中央演算処理装置（メインCPU:Central Processing Unit）106、RAM(Random Access Memory)107、ROM(Read Only Memory)108、AV処理部109、入力インターフェース110、PIO(パラレルI/Oインターフェース)111、SIO(シリアルI/Oインターフェース)112を備えている。【0056】記録再生器300本体の制御系として機能する構成部であり、主として記録再生器暗号処理部302で復号されたデータの再生を実行する再生処理部として機能する。例えば中央演算処理装置（メインCPU:Central Processing Unit）106は、制御部301の制御のもとに記録デバイスから読み出されて復号されたコンテンツデータをAV処理部109へ出力する等、コンテンツの再生、実行に関する制御を行なう。【0057】RAM107は、種処理用の主記憶メモリとして使用され、メインCPU106による処理のための作業領域として使用される。ROM108は、メインCPU106で起動されるOS等を立ち上げるための基本プログラム等が格納される。MPEG2デコーダ、ATRACデコーダ、MP3デコーダ等のデータ圧縮伸長処理機構を有し、記録再生器本体に付属または接続された図示しないディスプレイまた

はスピーカ等のデータ出力機器に対するデータ出力のための処理を実行する。【0059】入力インターフェース110は、コントローラ、キーボード、マウス等、各種の入力手段からの入力データをメインCPU106に出力する。メインCPU106は、例えば実行中のゲームプログラム等に基づいて使用者からのコントローラからの指示に従った処理を実行する。【0060】PIO(パラレルI/Oインターフェース)111、SIO(シリアルI/Oインターフェース)112は、メモリカード、ゲームカートリッジ等の記憶装置、携帯用電子機器等との接続インターフェースとして使用される。【0061】また、メインCPU106は、例えば実行中のゲーム等に関する設定データ等をセーブデータとして記録デバイス400に記憶する際の制御も行なう。この処理の際には、記憶データを制御部301に転送し、制御部301は必要に応じて暗号処理部302にセーブデータに関する暗号処理を実行させ、暗号化データを記録デバイス400に格納する。これらの暗号処理については、後段で詳細に説明する。【0062】記録デバイス400は、ましくは記録再生器300に対して着脱可能な記憶媒体であり、例えばメモリカードによって構成される。記録デバイス400は暗号処理部401、外部メモリ402を有する。【0063】記録デバイス暗号処理部401は、記録再生器300からのコンテンツデータのダウンロード、または記録デバイス400から記録再生器300へのコンテンツデータの再生処理時等における記録再生器300と記録デバイス400間の相互認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する処理部であり、記録再生器300の暗号処理部と同様、制御部、内部メモリ、暗号/復号化部等を有する。これらの詳細は図3に示す。外部メモリ402は、前述したように、例えばEEPROM等のフラッシュメモリからなる不揮発メモリ、ハードディスク、電池つきRAMなどによって構成され、暗号化されたコンテンツデータ等を格納する。【0064】図3は、本発明のデータ処理装置がデータ供給を受けるコンテンツ提供手段であるメディア500、通信手段600から入力されるデータ構成の概略を示すとともに、これらコンテンツ提供手段500、600からコンテンツを入力する記録再生器300と、記録デバイス400における暗号処理に関する構成を中心として、その構成を示した図である。【0065】メディア500は、磁気ディスクメディア、磁気テープメディア、半導体メディア等である。通信手段600は、インターネット通信、ケーブル通信、衛星通信等の、データ通信可

能な手段である。【0066】図3において、記録再生器テンツ提供手段であるメディア500、通信手段600から入力されるデータ、すなわち図3に示すような所定のフォーマットに従ったコンテンツを検証し、検証後にコンテンツを記録デバイス400に保存する。【0067】分に示すようにコンテンツデータは以下のような構成部を有する。識別情報：コンテンツデータの識別子としての報。取扱方針：コンテンツデータの構成情報、例えばコンテンツデータを構成するヘッダ一部サイズ、コンテンツ部サイズ、フォーマットのバージョン、コンテンツがプログラムかデータか等を示すコンテンツタイプ、さらにコンテンツがダウンロードした機器だけでしか利用できないのか他の機器でも利用できるのか等の利用制限情報等を含む取扱方針。ブロック情報：コンテンツブロックの数、暗号化の有無を示す暗号化フラグ等から構成されるブロック情報。鍵データ：上述のブロック情報を暗号化するいはコンテンツブロックを暗号化するコンテンツ鍵等からなる鍵データ。コンテンツブロック：実際の再生データ、音楽、画像データ等からなるコンテンツブロック。を有する。なお、コンテンツデータ詳細については、段で図4以下を用いてさらに詳細に説明する。【0068】では、これをコンテンツ鍵 (Content Key (以下、K_{co}nとする)) と呼ぶ) によって暗号化されて、メディア500、通信手段600から記録再生器300に提供される。コンテンツは、記録再生器300を介して記録デバイス400の外部メモリに格納することができる。イス内の内部メモリ405に格納された記録デバイス固有の鍵 (ここでは、これを保存鍵 (Storage Key (以下、K_{st}rとする)) と呼ぶ) を用いて、コンテンツデータに含まれるコンテンツ、及びコンテンツデータのヘッダ情報として含まれるブロック情報、各種鍵情報、例えばコンテンツ鍵K_{co}nなどを暗号化して外部メモリ402に記憶する。コンテンツデータの記録再生器300から記録デバイス400へのダウンロード処理、あるいは記録再生器300による記録デバイス400内に格納されたコンテンツデータの再生処理においては、機器間の相互認証処理、コンテンツデータの暗号化、復号化処理等、所定の手続きが必要となる。これらの処理については、後段で詳細に説明する。【0070】記録デ

暗号処理部401、外部メモリ402を有し、暗号処理部401は、制御部403、通信部404、内部メモリ405、暗号/復号化部406、外部メモリ制御部407を有する。【0071】記録デバイス400は、暗号処理全般を囲り、外部メモリ402を制御するとともに、記録再生器300からのコマンドを解釈し、処理を実行する記録デバイス暗号処理部401と、コンテンツなどを保持する外部メモリ402からなる。【0072】記録デバイス暗号処理部401全体を制御する制御部403、記録再生器300とデータの送受信を行う通信部404、暗号処理用の鍵データなどの情報を保持し、外部から容易に読み出せないように処理が施された内部メモリ405、暗号化処理、復号化処理、認証用のデータの生成・検証、乱数の発生などを行う暗号/復号化部406、外部メモリ402のデータを読み書きする外部メモリ制御部407を有する。【0073】制御部403は、記録デバイスにおいて実行される認証処理、暗号化/復号化処理等の暗号処理全般に係る制御を実行する制御部であり、例えば、記録再生器300と記録デバイス400との間で実行される認証処理の完了時における認証完了フラグの設定、暗号処理部401の暗号/復号化部406において実行される各種処理、例えばダウンロード、あるいは再生コンテンツデータに関するチェック値生成処理の実行命令、各種鍵データの生成処理の実行命令等、暗号処理全般に関する制御を行なう。【0074】内部メモリ405は、後述するが、複数のブロックを持つメモリによって構成されており、記録デバイス400において実行される相互認証処理、チェック値照合処理、暗号化、復号化処理等、各種処理において必要となる鍵データ、あるいは識別データ等の組を複数格納した構成となっている。【0075】記録デバイス405は、先に説明した記録再生器暗号処理部302の内部メモリ307と同様、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しが容易な構造にしておく必要がある。従って、記録デバイス400の暗号処理部401は、外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または/又は周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性とした構成とされる。なお、記録再生器暗号処理部302は、鍵などの秘密の情報を容易に外部に漏らさないように構成されたソフトウェアであってもよい。【0076】暗号/復号化部406は、記録再生器300からのコンテンツデータのダウンロード処理、記録デ

バイス400の外部メモリ402に格納されたコンテンツデータの再生処理、あるいは、記録再生器300と記録デバイス400間の相互認証処理の際、内部メモリ405に格納された鍵データ等を使用して、データの検証処理、暗号化処理、復号化処理、所定のチェック値や電子署名の生成・検証、乱数の発生などの処理等を実行する。【0077】通信部404は、記録再生器300の記録デバイスコントローラ303に接続され、記録再生器300の制御部301、あるいは、記録デバイス403の制御部403の制御に従って、コンテンツデータのダウンロード処理、再生処理、あるいは、相互認証処理の際の記録再生器300と記録デバイス400間の転送データの通信を行なう。【0078】(2)コンテンツデータフォーマットを示す図であり、図5に示す構成がコンテンツデータのヘッダ部の一部を構成する「取扱方針」の詳細を示す図であり、図6に示す構成がコンテンツデータのヘッダ部の一部を構成する「ブロック情報」の詳細を示す図である。【0079】図4に示す構成がコンテンツデータフォーマットを示す図であり、図5に示す構成がコンテンツデータのヘッダ部の一部を構成する「取扱方針」の詳細を示す図であり、図6に示す構成がコンテンツデータのヘッダ部の一部を構成する「ブロック情報」の詳細を示す図である。【0080】なお、ここでは、本発明のシステムに適用されるデータフォーマットの代表的な一例について説明するが、本発明のシステムでは、例えばゲームプログラムに対応したフォーマット、音楽データ等のリアルタイム処理に適したフォーマット等、異なる複数のデータフォーマットが利用可能であり、これらのフォーマットの構造については、後段「(10)複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理」において、さらに詳しく述べる。【0081】図4に示すデータフォーマットにおいて、グレーで示す部分は暗号化されたデータであり、二重枠の部分は改竄チェックデータ、他の白い部分は暗号化されていない平文のデータである。暗号化部の暗号化鍵は、それぞれの枠の左に示す鍵である。図4に示す例においては、コンテンツ部の各ブロック(コンテンツブロックデータ)に暗号化されたものと暗号化されていないものとが混在している。これらの形態は、コンテンツデータに応じて異なるものであり、データに含まれるすべてのコンテンツブロックデータが暗号化されている構成であってもよい。【0082】図4に示すように、データ部は、ヘッダ一部とコンテンツ部に分かれており、ヘッダ一部は、識別情報(Content ID)、取扱方針(Usage Policy)、チェック値A(Integrity Check Value A)

(以下、ICVaとする)、ブロック情報鍵(Block Information Table Key(以下、Kbitとする))、コンテンツ鍵Kcon、ブロック情報(Block Information Table(以下、BITとする))、チェック値B(ICVb)、総チェック値(ICVt)により構成されており、コンテンツ部は、複数のコンテンツブロック(例えば暗号化されたコンテンツと、暗号化されていないコンテンツ)から構成されている。【0083】ここで、識別情報をための個別の識別子(Content ID)を示している。取扱方針は、図5にその詳細を示すように、ヘッダ一部のサイズを示すヘッダーサイズ(Header Length)、コンテンツ部分のサイズを示すコンテンツサイズ(Content Length)、フォーマットのバージョン情報ムにおける示すフォーマットバージョン(Format Version)、フォーマットの種類を示すフォーマットタイプ(Format Type)、コンテンツ部に保存されているコンテンツがプログラムなのか、データなのか等コンテンツの種類を示すコンテンツタイプ(Content Type)、コンテンツタイプがプログラムである場合の起動優先順位を示す起動優先順位情報(Operation Priority)、このフォーマットに従ってダウンロードされたコンテンツが、ダウンロードした機器だけしか利用できないのか、他の同様な機器でも利用できるのかを示す利用制限情報(LocalizationField)、このフォーマットに従ってダウンロードされたコンテンツが、ダウンロードした機器から他の同様な機器に複製できるのか否かを示す複製制限情報(Copy Permission)、このフォーマットに従ってダウンロードされたコンテンツが、ダウンロードした機器から他の同様な機器に移動できるのか否かを示す移動制限情報(Move Permission)、コンテンツ部内のコンテンツブロックを暗号するのに使用したアルゴリズムを示す暗号アルゴリズム(Encryption Algorithm)、コンテンツ部内のコンテンツを暗号化するのに使用したアルゴリズムの使用方法を示す暗号化モード(Encryption Mode)、チェック値の生成方法を示す検証方法(Integrity Check Method)から構成されている。【0084】なお、上述した取扱項目は、1つの例であり、対応するコンテンツデータの構造に応じて様々な取扱方針情報を記録することが可能である。例えば後段の「(17)不正機器の排除(リボルバーフケーション)構成」で詳しく述べるが、不正な記録再生器の識別子をデータとして記録して、利用開始時の照合によって不正機器によるコンテンツ利用を排除するように構成することも可能である。【0085】チェック値A、ICVaの改竄を検証するためのチェック値である。コンテンツデータ全体ではなく部分データのチェック値、すなわち部分チェック値として機能する。データブロック情報鍵Kbitは、ブロック情報を暗号化するのに用い

られ、コンテンツ鍵 K_{con} は、コンテンツブロックを暗号化するのに用いられる。なお、ブロック情報鍵 K_{bit} 及びコンテンツ鍵 K_{con} は、メディア 500 上および通信手段 600 上では後述する配送鍵 (Distribution Key (以下、 K_{dis} とする)) で暗号化されている。【0086】ブロック情報の詳細を図 6 に示す。なお、図 6 のブロック情報は、図 4 から理解されるようにすべてブロック情報鍵 K_{bit} によって暗号化されているデータである。ブロック情報は、図 6 に示すように、コンテンツブロックの数を示すコンテンツブロック数 (Block Number) と N 個のコンテンツブロック情報から構成されている。コンテンツブロック情報は、ブロックサイズ (Block Length) 、暗号化されているか否かを示す暗号化フラグ (Encryption Flag) 、チェック値を計算する必要があるか否かを示す検証対象フラグ (ICV Flag) 、コンテンツチェック値 (ICVi) から構成されている。【0087】コンテンツチェック値は、各コンテンツロックの改竄を検証するために用いられるチェック値である。コンテンツチェック値の生成手法の具体例については、後段の「(10) 複数のデータフォーマットと、各フォーマットに対応する記録デバイスへのダウンロード処理および記録デバイスからの再生処理」の欄で説明する。なお、ブロック情報を暗号化しているブロック情報鍵 K_{bit} は、さらに、配送鍵 K_{dis} によって暗号化されている。【0088】図 4 のデータフォーマットのデータである。チェック値 B 、ICVb は、ブロック情報鍵 K_{bit} 、コンテンツ鍵 K_{con} 、ブロック情報の改竄を検証するためのチェック値である。コンテンツデータ全体ではなく部分データのチェック値、すなわち部分チェック値として機能する。総チェック値 ICVt は、ICVa、ICVb、各コンテンツブロックのチェック値 ICVi (設定されている場合)、これらの部分チェック値、あるいはそのチェック対象となるデータ全ての改竄を検証するためのチェック値である。【0089】なお、暗号化フラグ、検証対象フラグを自由に設定できるようにしているが、ある程度ルールを決めた構成としてもよい。例えば、暗号文領域と平文領域を固定サイズ繰り返しにしたり、全コンテンツデータを暗号化したりし、ブロック情報 BIT を圧縮してもよい。また、コンテンツ鍵 K_{con} をコンテンツブロック毎に異なるようにするため、コンテンツ鍵 K_{con} をヘッダー部分ではなく、コンテンツブロックに含ませるようにしてよい。コンテンツデータフォーマットの例については、「(10) 複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理」の項目において、さらに詳細に説明する。

【0090】(3) 本発明のデータ処理装置において適用可能な暗号処理概要次に、本発明のデータ処理装置において適用可能な暗号処理の態様について説明する。なお、本項目「(3) 本発明のデータ処理装置において適用可能な暗号処理の概要」に示す暗号処理に関する説明は、後段で具体的に説明する本発明のデータ処理装置における各種処理、例えば a. 記録再生器と記録デバイス間での認証処理。b. コンテンツの記録デバイスに対するダウンロード処理。c. 記録デバイスに格納したコンテンツの再生処理等の処理において実行される処理の基礎となる暗号処理の態様について、その概要を説明するものである。記録再生器 300 と記録デバイス 400 における具体的な処理については、本明細書の項目 (4) 以下において、各処理毎に詳細に説明する。【0091】以下、データ処理装置の暗号処理の概要について、(3-1) 共通鍵暗号方式によるメッセージ認証まず、共通鍵暗号方式を用いた改竄検出データの生成処理について説明する。改竄検出データは、改竄の検出を行ないたいデータに付け、改竄のチェックおよび作成者認証をするためのデータである。【0093】例えば、図 4 で説明した重枠部分の各チェック値 A 、 B 、総チェック値、および図 6 に示すブロック情報中の各ブロックに格納されたコンテンツチェック値等が、この改竄検出データとして生成される。【0094】ここでは、電子署名データの生成処理方法の例の 1 つとして共通鍵暗号方式における DES を用いた例を説明する。なお、本発明においては、DES 以外にも、同様の共通鍵暗号方式における処理として例えば F E A L (Fast Encipherment ALgorithm: NTT)、A E S (Advanced Encryption Standard: 米国次期標準暗号) 等を用いることも可能である。【0095】一般的な DES の処理を図 7 を用いて説明する。まず、電子署名を生成するに先立ち、電子署名の対象となるメッセージを 8 バイト単位に分割する (以下、分割されたメッセージを M_1 、 M_2 、 \dots 、 M_N とする)。そして、初期値 (Initialization Vector: IV) においては、ブロックサイズ、

1 Value (以下、 I Vとする)) と M 1 を排他的論理和する (その結果を I 1 とする) 。次に、 I 1 を D E S 暗号化部に入れ、鍵 (以下、 K 1 とする) を用いて暗号化する (出力を E 1 とする) 。続けて、 E 1 および M 2 を排他的論理和し、その出力 I 2 を D E S 暗号化部へ入れ、鍵 K 1 を用いて暗号化する (出力 E 2) 。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきた E N が電子署名になる。この値は一般にはメッセージ認証符号 (M A C (Message Authentication Code)) と呼ばれ、メッセージの改竄チェックに用いられる。また、このように暗号文を連鎖させる方のことを C B C (Cipher Block Chaining) モードと呼ぶ。【0 0 9 6】なお、図 7 のような生成例において出力される M A C 値が、図 4 で示すデータ構造中の二重枠部分の各チェック値 A, B 、総チェック値、および図 6 に示すブロック情報中の各ブロックに格納されたコンテンツチェック値 I C V 1 ~ I C V N として使用可能である。この M A C 値の検証時には、検証者が生成時と同様の方法で M A C 値を生成し、同一の値が得られた場合、検証成功とする。【0 0 9 7】なお、図 7 に示す例では初期値 I V 0 に 8 バイトメッセージ M 1 に排他的論理和したが、初期値 I V = 0 として、初期値を排他的論理和しない構成とすることも可能である。【0 0 9 8】図 7 に示す M A C 値生成方法を示す処理構成図を図 8 に示す。図 8 は、図 7 のシングル D E S に代えてトリプル D E S (Triple D E S) を用いて M A C 値の生成を実行する例を示したものである。【0 0 9 9】図 9 に示す D E S 構成部の詳細構成例を図 9 に示す。図 9 (a) 、 (b) に示すようにトリプル D E S (Triple D E S) としての構成には 2 つの異なる様がある。図 9 (a) は、 2 つの暗号鍵を用いた例を示すものであり、鍵 1 による暗号化処理、鍵 2 による復号化処理、さらに鍵 1 による暗号化処理の順に処理を行う。鍵は、 K 1 、 K 2 、 K 1 の順に 2 種類用いる。図 9 (b) は 3 つの暗号鍵を用いた例を示すものであり、鍵 1 による暗号化処理、鍵 2 による暗号化処理、さらに鍵 3 による暗号化処理の順に処理を行い 3 回とも暗号化処理を行う。鍵は、 K 1 、 K 2 、 K 3 の順に 3 種類の鍵を用いる。このように複数の処理を連続させる構成とすることで、シングル D E S に比較してセキュリティ強度を向上させている。しかしながら、このトリプル D E S (Triple D E S) 構成は、処理時間がシングル D E S のおよそ 3 倍かかるという欠点を有する。【0 1 0 0】図 8 および図 9 で説明した構成を改良した M A C 値生成構成例を図 10 に示す。図 10 においては、署名対象となるメッセージ列の初めか

ら途中までの各メッセージに対する暗号化処理は全てシングル D E S による処理とし、最後のメッセージに対する暗号化処理のみを図 9 (a) に示すトリプル D E S (Triple D E S) 構成としたものである。【0 1 0 1】図 10 において、メッセージの M A C 値の生成処理時間は、シングル D E S による M A C 値生成処理に要する時間とほぼ同程度に短縮され、かつセキュリティはシングル D E S による M A C 値よりも高めることが可能となる。なお、最終メッセージに対するトリプル D E S 構成は、図 9 (b) の構成とすることも可能である。【0 1 0 2】(3-2) 公開鍵暗号の場合の電子署名データの生成方法であるが、次に、暗号化方式として公開鍵暗号方式を用いた電子署名の生成方を図 11 を用いて説明する。図 11 に示す処理は、 E C - D S A ((Elliptic Curve Digital Signature Algorithm) 、 IEEE P1363/D3) を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として椭円曲線暗号 (Elliptic Curve Cryptography (以下、 E C C と呼ぶ)) を用いた例を説明する。なお、本発明のデータ処理装置においては、椭円曲線暗号以外に同様の公開鍵暗号方式における、例えば R S A 暗号 ((Rivest, Shamir, Adleman) など (ANSI X9.31)) を用いることも可能である。【0 1 0 3】図 11 の各ステップについて、 S 1 において、 p を標数、 a, b を椭円曲線の係数 (椭円曲線 : $y^2 = x^3 + ax + b$) 、 G を椭円曲線上のベースポイント、 r を G の位数、 K s を秘密鍵 ($0 < K_s < r$) とする。ステップ S 2 において、メッセージ M のハッシュ値を計算し、 $f = \text{Hash}(M)$ とする。【0 1 0 4】ここで、ハッシュを求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値 (出力) から入力を予測することが難しく、ハッシュ関数に入力されたデータの 1 ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、 M D 4 、 M D 5 、 S H A - 1 などが用いられる場合もあるし、図 7 他で説明したと同様の D E S - C B C が用いられる場合もある。この場合は、最終出力値となる M A C (チェック値 : I C V に相当する) がハッシュ値となる。【0 1 0 5】続けて、ステップ S 3 で、乱数 u ($0 < u < r$) を生成し、ステップ S 4 でベースポイントを u 倍した座標 V (X v , Y v) を計算する。なお、椭円曲線上の加算、 2 倍算は次のように定義されている。【0 1 0 6】

【数1】

$P=(X_a, Y_a), Q=(X_b, Y_b), R=(X_c, Y_c)=P+Q$ とすると、
 $P \neq Q$ の時 (加算)、
 $X_c = \lambda^3 - X_a - X_b$
 $Y_c = \lambda \times (X_a - X_c) - Y_a$
 $\lambda = (Y_b - Y_a) / (X_b - X_a)$
 $P=Q$ の時 (2倍算)、
 $X_c = \lambda^3 - 2X_a$
 $Y_c = \lambda \times (X_a - X_c) - Y_a$
 $\lambda = (3(X_a)^2 + a) / (2Y_a)$

【0107】これらを用いて点Gのu倍を計算する (速度は遅いが、最もわかりやすい演算方法として次のように行う。G、 $2 \times G$ 、 $4 \times G \dots$ を計算し、uを2進数展開して1が立っているところに対応する $2^i \times G$ (Gをi回2倍算した値) を加算する (iはuのLSBから数えた時のビット位置))。【0108】ステップS5で、 $c = X$ み、電子署名が正しいと判定する。【0109】ステップS6でこの値が0になるかどうか判定し、0でなければステップS7で $d = [(f + cK_s) / u] \bmod r$ を計算し、ステップS8でdが0であるかどうか判定し、dが0でなければ、ステップS9でcおよびdを電子署名データとして出力する。仮に、rを160ビット長の長さであると仮定すると、電子署名データは320ビット長となる。【0110】(3-3) の検証次に、公開鍵暗号方式を用いた電子署名の検証方法について説明する。ステップS11で、Mをメッセージ、pを標数、a、bを楕円曲線の係数 (楕円曲線: $y^2 = x^3 + ax + b$)、Gを楕円曲線上のベースポイント、rをGの位数、GおよびKs × Gを公開鍵 ($0 < K_s < r$) とする。ステップS12で電子署名データcおよびdが $0 < c < r$ 、 $0 < d < r$ を満たすか検証する。これを満たしていた場合、ステップS13で、メッセージMのハッシュ値を計算し、 $f = H_a s h(M)$ とする。次に、ステップS14で $h = 1/d \bmod r$ を計算し、ステップS15で $h_1 = f h \bmod r$ 、 $h_2 = c h \bmod r$ を計算する。【0111】ステップS16において、 h_1 および h_2 を用い、点 $P = (X_p, Y_p) = h_1 \times G + h_2 \cdot K_s \times G$ を計算する。電子署名検証者は、公開鍵GおよびKs × Gを知っているので、図11のステップS4と同様に楕円曲線上の点のスカラ一倍の計算ができる。そして、ステップS17で点Pが無限遠点かどうか判定し、無限遠点でなければステップS18に進む (実際には、無限遠点の判定はステップS16でできて

しまう。つまり、 $P = (X, Y)$ 、 $Q = (X, -Y)$ の加算を行うと、 λ が計算できず、 $P + Q$ が無限遠点であることが判明している)。ステップS18で $X_p \bmod r$ を計算し、電子署名データcと比較する。最後に、この値が一致していた場合、ステップS19に進み、電子署名が正しいと判定する。【0112】電子署名が正しいとは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。【0113】ステップcまたはdが、 $0 < c < r$ 、 $0 < d < r$ を満たさなかつた場合、ステップS20に進む。また、ステップS17において、点Pが無限遠点であった場合もステップS20に進む。さらにまた、ステップS18において、 $X_p \bmod r$ の値が、電子署名データcと一致していないか、または改竄された場合にもステップS20に進む。【0114】ステップS20でデータは改竄されているか、公開/公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。【0115】(3-4) 共通鍵暗号方式を用いて説明する。図13において、共通鍵暗号方式としてDESを用いているが、前述のように同様な共通鍵暗号方式であればいずれでもよい。図13において、まず、Bが64ビットの乱数Rbを生成し、Rbおよび自己のIDであるID(b)をAに送信する。これを受信したAは、新たに64ビットの乱数Raを生成し、Ra、Rb、ID(b)の順に、DESのCBCモードで鍵Ka bを用いてデータを暗号化し、Bに返送する。図7に示すDESのCBCモード処理構成によれば、RaがM1、RbがM2、ID(b)がM3に相当し、初期値:既IV=0としたときの出力E1、E2、E3が暗号文となる。【0116】これを受信したBは、受信データを鍵Ka bで復号化する。受信データの復号化方法は、まず、暗号文E1を鍵Ka bで復号化し、乱数Raを得る。次に、暗号文E2を鍵Ka bで復号化し、その結果とE1を排他的論理和し、Rbを得る。最後に、暗号文E3を鍵Ka bで復号化し、その結果とE2を排他的論理和

し、ID(b)を得る。こうして得られたR_a、R_b、ID(b)の内、R_bおよびID(b)が、Bが送信したものと一致するか検証する。この検証に通った場合、BはAを正当なものとして認証する。【0117】次にBは、認証後成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。なお、電子署名の検証方法については、図12で説明したのでその詳細は省略する。【0118】(3-6)より暗号を用いた相互認証方法を、図15を用いて説明する。図15において、公開鍵暗号方式としてECCを用いているが、前述のように同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも160ビットでなくてもよい。図15において、まずBが、64ビットの乱数R_bを生成し、Aに送信する。これを受信したAは、新たに64ビットの乱数R_aおよび標数pより小さい乱数A_kを生成する。そして、ベースポイントGをA_k倍した点A_v=A_k×Gを求め、R_a、R_b、A_v(X座標とY座標)に対する電子署名A_{sig}を生成し、Aの公開鍵証明書とともにBに返送する。ここで、R_aおよびR_bはそれぞれ64ビット、A_vのX座標とY座標がそれぞれ160ビットであるので、合計448ビットに対する電子署名を生成する。電子署名の生成方法は図11で説明したので、その詳細は省略する。また、公開鍵証明書も図14で説明したので、その詳細は省略する。【0120】(3-5) 公開鍵証明書は、公開鍵暗号方式における認証局(CA: Certificate Authority)が発行する証明書であり、ユーザが自己のID、公開鍵等を認証局に提出することにより、認証局側が認証局のIDや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。【0121】図14に示す公開鍵証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前(ユーザID)、証明書利用者の公開鍵並びに電子署名を含む。【0122】電子署名は、証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。この電子署名の生成には、例えば図11で説明した処理フローが適用される。【0123】認証局は、図14に示す公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布(これをリボケーション:Revocationと呼ぶ)を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

【0124】一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。なお、電子署名の検証方法については、図12で説明したのでその詳細は省略する。【0125】(3-6)より暗号を用いた相互認証方法を、図15を用いて説明する。図15において、公開鍵暗号方式としてECCを用いているが、前述のように同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも160ビットでなくてもよい。図15において、まずBが、64ビットの乱数R_bを生成し、Aに送信する。これを受信したAは、新たに64ビットの乱数R_aおよび標数pより小さい乱数A_kを生成する。そして、ベースポイントGをA_k倍した点A_v=A_k×Gを求め、R_a、R_b、A_v(X座標とY座標)に対する電子署名A_{sig}を生成し、Aの公開鍵証明書とともにBに返送する。ここで、R_aおよびR_bはそれぞれ64ビット、A_vのX座標とY座標がそれぞれ160ビットであるので、合計448ビットに対する電子署名を生成する。電子署名の生成方法は図11で説明したので、その詳細は省略する。また、公開鍵証明書も図14で説明したので、その詳細は省略する。【0126】Aの公開鍵証明書、R_a、R_b、A_v、電子署名A_{sig}を受信したBは、Aが送信してきたR_bが、Bが生成したものと一致するか検証する。その結果、一致していた場合には、Aの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Aの公開鍵を取り出す。公開鍵証明書の検証については、図14を用いて説明したので、その詳細は省略する。そして、取り出したAの公開鍵を用い電子署名A_{sig}を検証する。電子署名の検証方法は図12で説明したので、その詳細は省略する。電子署名の検証に成功した後、BはAを正当なものとして認証する。【0127】次に、Bは、標数pより小さい乱数A_kを生成する。そして、ベースポイントGをB_k倍した点B_v=B_k×Gを求め、R_b、R_a、B_v(X座標とY座標)に対する電子署名B_{sig}を生成し、Bの公開鍵証明書とともにAに返送する。【0128】Bの公開鍵証明書、電子署名B_{sig}を受信したAは、Bが送信してきたR_aが、Aが生成したものと一致するか検証する。その結果、一致していた場合には、Bの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Bの公開鍵を取り出す。そして、取り出したBの公開鍵を用い電子署名B_{sig}を検証する。電子署名の検証に成功した後、Aは

Bを正当なものとして認証する。【0129】両者が認証に成 $K_s \times G$ とすることで、暗号化に使用する鍵と復号化に $\times A_k$ （ B_k は乱数だが、 A_v は楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、 A は $A_k \times B_v$ を計算し、これら点のX座標の下位64ビットをセッション鍵として以降の通信に使用する（共通鍵暗号を64ビット鍵長の共通鍵暗号とした場合）。もちろん、Y座標からセッション鍵を生成してもよいし、下位64ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。【0130】電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。【0131】（3-7）理次に、楕円曲線暗号を用いた暗号化について、図16を用いて説明する。ステップS21において、 M_x, M_y をメッセージ、 p を標数、 a, b を楕円曲線の係数（楕円曲線： $y^2=x^3+ax+b$ ）、 G を楕円曲線上のベースポイント、 r を G の位数、 G および $K_s \times G$ を公開鍵（ $0 < K_s < r$ ）とする。ステップS22で乱数 u を $0 < u < r$ になるように生成し、ステップS23で公開鍵 $K_s \times G$ を u 倍した座標 V を計算する。なお、楕円曲線上のスカラー倍は図11のステップS4で説明したので、詳細は省略する。ステップS24で、 V のX座標を M_x 倍して p で剰余を求め X_0 とし、ステップS25で V のY座標を M_y 倍して p で剰余を求め Y_0 とする。なお、メッセージの長さが p のビット数より少ない場合、 M_y は乱数を使い、復号化部では M_y を破棄するようする。ステップS26において、 $u \times G$ を計算し、ステップS27で暗号文 $u \times G, (X_0, Y_0)$ を得る。【0132】理次に、楕円曲線暗号を用いた復号化について、図17を用いて説明する。ステップS31において、 $u \times G, (X_0, Y_0)$ を暗号文データ、 p を標数、 a, b を楕円曲線の係数（楕円曲線： $y^2=x^3+ax+b$ ）、 G を楕円曲線上のベースポイント、 r を G の位数、 K_s を秘密鍵（ $0 < K_s < r$ ）とする。ステップS32において、暗号データ $u \times G$ を秘密鍵 K_s 倍し、座標 V （ X_v, Y_v ）を求める。ステップS33では、暗号データの内、 (X_0, Y_0) のX座標を取り出し、 $X_1 = X_0 \mod p$ を計算し、ステップS34においては、Y座標を取り出し、 $Y_1 = Y_0 \mod p$ を計算する。そして、ステップS35で X_1 を M_x とし、 Y_1 を M_y としてメッセージを取り出す。この時、 M_y をメッセージにしていなかった場合、 Y_1 は破棄する。【0133】このように、秘密鍵を K_s 、公開鍵を G 、

使用する鍵を、異なる鍵とすることができます。【0134】また、暗号が知られているが、詳しい説明は省略する（PKCS #1 Version2に詳細が記述されている）。【0135】（3-9）舌法としては、熱雑音を増幅し、そのA/D出力から生成する真性乱数生成法や、M系列等の線形回路を複数組み合わせて生成する疑似乱数生成法等が知られている。また、DES等の共通鍵暗号を用いて生成する方法も知られている。本例では、DESを用いた疑似乱数生成方法について説明する（ANSI X9.17ベース）。【0136】まず、時限（これ以下のビット数の場合、上位ビットを0とする）の値をD、Triple-DESに使われる鍵情報を K_r 、乱数発生用の種（Seed）をSとする。このとき、乱数Rは以下のように計算される。【0137】【数2】

$$I = \text{Triple-DES}(K_r, D) \quad \dots \dots \dots (2-1)$$

$$R = \text{Triple-DES}(K_r, S \wedge I) \quad \dots \dots \dots (2-2)$$

$$S = \text{Triple-DES}(K_r, R \wedge I) \quad \dots \dots \dots (2-3)$$

【0138】ここで、Triple-DES()は、第1引数を暗号鍵情報として、第2引数の値をTriple-DESで暗号化する関数とし、演算 \wedge は64ビット単位の排他的論理和、最終的に得た値Sは、新規のSeed（種）として更新されていくものとする。【0139】（2-2）式、（2-3）式を繰り返すものとする。【0140】用可能な暗号処理に関する各種処理態様について説明した。次に、本発明のデータ処理装置において実行される具体的な処理について、詳細に説明する。【0141】（4）記録暗号処理部302に構成された内部メモリ307のデータ保持内容を説明する図である。【0142】図18に示すように、以下の鍵、データが格納されている。MKake：記録再生器300と記録デバイス400（図3参照）との間で実行される相互認証処理に必要な認証鍵（Authentication and Key Exchange Key（以下、Kakeとする））を生成するための記録デバイス認証鍵用マスター鍵。IVake：記録デバイス認証鍵用初期値。MKdis：配達マスター鍵。IVdis：配達鍵生成用初期値。Kicva：チ

$$Kake = DES(MKake, IDmem^* IVake)$$

【0150】ここで、MKakeは、記録再生器300と記録デバイス400(図3参照)との間で実行される相互認証処理に必要な認証鍵Kakeを生成するための記録デバイス認証鍵用マスター鍵であり、これは、前述したように記録再生器300の内部メモリ307に格納されている鍵である。またIDmemは、記録デバイス

400に固有の記録デバイス識別情報である。さらに I
V a k e は、記録デバイス認証鍵用初期値である。ま
た、上記式において、D E S () は、第1引数を暗号鍵
として、第2引数の値をD E Sで暗号化する関数であ
り、演算 ^ は64ビット単位の排他的論理和を示す。【0151】

する場合には、図7、8に示されるメッセージMを記録デバイス識別情報：IDmemとし、鍵K1をデバイス認証鍵用マスター鍵：MKakeとし、初期値IVを：IVakeとして得られる出力が認証鍵Kakeとなる。【0152】次に、ステップS47で相互認証およびセッション鍵Ksesの生成処理を行う。相互認証は、記録再生器暗号処理部302の暗号／復号化部308と記録デバイス暗号処理部401の暗号／復号化部406の間で行われ、その仲介を記録再生器300の制御部301が行っている。【0153】相互認証処理は、例えば前述の処理にしたがって実行することができる。図13に示す構成において、A、Bがそれぞれ記録再生器300と記録デバイス400に対応する。まず、記録再生器300の記録再生器暗号処理部302が乱数Rbを生成し、乱数Rbおよび自己のIDである記録再生器識別情報IDdevを記録デバイス400の記録デバイス暗号処理部401に送信する。なお、記録再生器識別情報IDdevは、記録再生器300内に構成された記憶部に記憶された再生器固有の識別子である。記録再生器暗号処理部302の内部メモリ中に記録再生器識別情報IDdevを記録する構成としてもよい。【0154】乱数Rbを受信した記録デバイス400の記録デバイス暗号処理部401は、新たに64ビットの乱数Raを生成し、Ra、Rb、と記録再生器識別情報IDdevの順に、DESのCBCモードで認証鍵Kakeを用いてデータを暗号化し、記録再生器300の記録再生器暗号処理部302に返送する。例えば、図7に示すDESのCBCモード処理構成によれば、RaがM1、RbがM2、IDdevがM3に相当し、初期値：IV=IVmemとしたときの出力E1、E2、E3が暗号文となる。【0155】暗号文E1、E2、E3を受信した記録再生器300の記録再生器暗号処理部302は、受信データを認証鍵Kakeで復号化する。受信データの復号化方法は、まず、暗号文E1を認証鍵Kakeで復号化し、その結果とIVmemとを排他的論理和し、乱数Raを得る。次に、暗号文E2を認証鍵Kakeで復号化し、その結果とE1を排他的論理和し、Rbを得る。最後に、暗号文E3を認証鍵Kakeで復号化し、その結果とE2を排他的論理和し、記録再生器識別情報IDdevを得る。こうして得られたRa、Rb、記録再生器識別情報IDdevの内、Rbおよび記録再生器識別情報IDdevが、記録再生器300が送信したものと一致するか検証する。この検証に通った場合、記録再生器300の記録再生器暗号処理部302は記録デバイス400を正当なものとして認証する。【0156】次に、記録再明において実行される認証処理手続きは、様々な処理が

処理部302は、認証後に使用するセッション鍵(Session Key (以下、Ksesとする))を生成する(生成方法は、乱数を用いる)。そして、Rb、Ra、Ksesの順に、DESのCBCモードで鍵Kake、初期値IVmemを用いて暗号化し、記録デバイス400の記録デバイス暗号処理部401に返送する。【0157】これを受信デバイス暗号処理部401は、受信データを鍵Kakeで復号化する。受信データの復号化方法は、記録再生器300の記録再生器暗号処理部302における復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたRb、Ra、Ksesの内、RbおよびRaが、記録デバイス400が送信したものと一致するか検証する。この検証に通った場合、記録デバイス400の記録デバイス暗号処理部401は記録再生器300を正当なものとして認証する。互いに相手を認証した後には、セッション鍵Ksesは、認証後の秘密通信のための共通鍵として利用される。【0158】なお、受信データの検証一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。【0159】相互認証に成功した場合には、48からステップS49に進み、セッション鍵Ksesをお記録再生器300の記録再生器暗号処理部302で保持するとともに、相互認証が終了したことを示す認証完了フラグをセットする。また、相互認証に失敗した場合には、ステップS50に進み、認証処理過程で生成されたセッション鍵Ksesを破棄するとともに、認証完了フラグをクリアする。なお、すでにクリアされている場合には必ずしもクリア処理は必要ではない。【0160】なお、記録デバイス挿入口から取り除かれた場合には、記録再生器300内の記録デバイス検知手段が、記録再生器300の制御部301に記録デバイス400が取り除かれたことを通知し、これを受けた記録再生器300の制御部301は、記録再生器300の記録再生器暗号処理部302に対し記録デバイス挿入口番号に対応する認証完了フラグをクリアするように命令し、これを受けた記録再生器300の記録再生器暗号処理部302は、記録デバイス挿入口番号に対応する認証完了フラグをクリアする。【0161】なお、手手続きにしたがって実行する例について説明したが、上述した認証処理例に限らず、例えば先に説明した図15の相互認証手続きに従った処理を実行してもよい。また、図13に示す手手続きにおいて、図13のAを記録再生器300とし、Bを記録デバイス400とし、B：記録デバイス400がA：記録再生器300に最初に送付するIDを記録デバイス中の鍵ブロック中の記録デバイス識別情報として相互認証処理を行なってもよい。本発明

適用可能であり、上述の認証処理に限定されるものではない。【0162】(6-2) 相互認証時の鍵ブロックの切り替え本発明のデータ処理装置における相互認証処理における1つの特徴は、記録デバイス400側に複数の鍵ブロック(e.g. N個の鍵ブロック)を構成して、記録再生器300が1つの鍵ブロックを指定(図20の処理フローにおけるステップS44)して認証処理を実行する点である。先に図19において説明したように、記録デバイス400の暗号処理部401に構成された内部メモリ405には複数の鍵ブロックが形成されており、それぞれが異なる鍵データ、ID情報等各種データを格納している。図20で説明した記録再生器300と記録デバイス400間で実行される相互認証処理は、図19の記録デバイス400の複数の鍵ブロックの1つの鍵ブロックに対して実行される。【0163】従来、記憶媒体とその再生機器における相互認証処理を実行する構成では、相互認証に用いる鍵:認証鍵は共通なものが使用されるのが一般的であった。従って、例えば製品仕向け先(国別)ごと、あるいは製品ごとに認証鍵を変更しようとすると、記録再生器側と、記録デバイス側の認証処理に必要となる鍵データを双方の機器において変更することが必要となる。従って例えば新たに発売された記録再生器に格納された認証処理に必要となる鍵データは、先に販売された記録デバイスに格納された認証処理に必要となる鍵データに対応せず、新たな記録再生器は、古いバージョンの記録デバイスへのアクセスができなくなってしまう事態が発生する。逆に新しいバージョンの記録デバイスと古いバージョンの記録再生器との関係においても同様の事態が発生する。【0164】本発明のデータ処理装置においては、図9に示すように予め記録デバイス400に複数の異なる鍵セットとしての鍵ブロックが格納されている。記録再生器は例えば製品仕向け先(国別)ごと、あるいは製品、機種、バージョン、アプリケーションごとに、認証処理に適用すべき鍵ブロック、すなわち指定鍵ブロックが設定される。この設定情報は、記録再生器のメモリ部、例えば、図3における内部メモリ307、あるいは、記録再生器300の有する他の記憶素子内に格納され、認証処理時に図3の制御部301によってアクセスされ設定情報にしたがった鍵ブロック指定が行われる。【0165】記録再生器300の内部メモリ307の記録デバイス認証鍵用マスター鍵MKakeは、それぞれの指定鍵ブロックの設定に従って設定された認証鍵用マスター鍵であり、指定鍵ブロックにのみ対応可能となっており、指定鍵ブロック以外の鍵ブロックとの相互認証は成立しない構成となっている。

【0166】図19から理解されるように、記録デバイス400の内部メモリ405には1~NのN個の鍵ブロックが設定され、各鍵ブロック毎に記録デバイス識別情報、認証鍵、初期値、保存鍵、乱数生成鍵、種が格納され、少なくとも認証用のかぎデータがブロック毎に異なるデータとして格納されている。【0167】このように、記録デバイスの鍵データ構成は、ブロック毎に異なっている。従って、例えば、ある記録再生機器Aが内部メモリに格納された記録デバイス認証鍵用マスター鍵MKakeを用いて認証処理を行ない得る鍵ブロックは鍵ブロックN o. 1であり、また別の仕様の記録再生器Bが認証可能な鍵ブロックは別の鍵ブロック、例えば鍵ブロックN o. 2のように設定することが可能となる。【0168】後段でさきを記録デバイス400の外部メモリ402に格納する再生機器、各鍵ブロックに格納された保存鍵Kstrを用いて暗号化処理がなされ、格納されることになる。より、具体的には、コンテンツブロックを暗号化するコンテンツ鍵を保存鍵で暗号化処理する。【0169】図19に示すように、毎に異なる鍵として構成されている。従って、異なる鍵ブロックを指定するように設定された2つの異なる設定の記録再生器間においては、ある1つの記録デバイスのメモリに格納されたコンテンツを両者で共通に利用することは防止される。すなわち、異なる設定のなされた記録再生器は、それぞれの設定に合致する記録デバイスに格納されたコンテンツのみが利用できる。【0170】なお、各鍵データは共通化することも可能であり、例えば認証用の鍵データ、保存鍵データのみを異なるように構成してもよい。【0171】このような記録デバイスに複数の異なる鍵データからなる鍵ブロックを構成する具体例としては、例えば記録再生器300の機種別(据え置き型、携帯型等)で指定すべき鍵ブロック番号を異なるように設定したり、あるいは、アプリケーション毎に指定鍵ブロックを異なるように設定する例がある。さらに、例えば日本で販売する記録再生器については指定鍵ブロックをN o. 1とし、米国で販売する記録再生器は指定鍵ブロックをN o. 2とするように地域ごとに異なる鍵ブロック設定を行なう構成とすることも可能である。このような構成とすることで、それぞれの異なる販売地域で使用され、記録デバイスに異なる保存鍵で格納されたコンテンツは、たとえメモリカードのような記録デバイスが米国から日本、あるいは日本から米国へ転送されても、異なる鍵設定のなされた記録再生器で利用することは不可能であるので、メモリに格納したコンテンツの不正、無秩序な流通を防止できる。具体的には、異なる保存鍵Kstrで暗号化されているコンテンツ鍵Kconが2

国間で相互に利用可能となる状態を排除することができる。【0172】さらに、図19に示す記録デバイス400の内部メモリ405の鍵ブロック1～Nまでの少なくとも1つの鍵ブロック、例えばN_o。Nの鍵ブロックをいずれの記録再生器300においても共通に利用可能な鍵ブロックとして構成してもよい。【0173】例えば、全ての鍵ブロックに対する認証可能なマスター鍵を格納する構成としたので、様々な利用態様に応じたコンテンツの利用制限を設定することが可能となる。【0177】なお、1つの能な鍵ブロックを複数、例えば1～kとし、他の記録再生器において指定可能な鍵ブロックをp～qのように複数とすることも可能であり、また、共通に利用可能な鍵ブロックを複数設ける構成としてもよい。【0178】(7)記録ダウンロード処理次に、本発明のデータ処理装置において、記録再生器400から記録デバイス400の外部メモリにコンテンツをダウンロードする処理について説明する。【0179】図22にデバイス400へコンテンツをダウンロードする手順を説明する流れ図である。なお、図22においては、既に記録再生器300と記録デバイス400との間で上述した相互認証処理が完了しているものとする。【0180】ステップS50の制御部301は、読み取り部304を使ってコンテンツを格納したメディア500から所定のフォーマットに従ったデータを読み出すか、通信部305を使って通信手段600から所定のフォーマットに従ってデータを受信する。そして、記録再生器300の制御部301は、データの内のヘッダ(Header)部分(図4参照)を記録再生器300の記録再生器暗号処理部302に送信する。【0181】次に、ステップS52において、ステップS51でヘッダ(Header)を受信した記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308にチェック値Aを計算させる。チェック値Aは、図23に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵K_ic_vaを鍵とし、識別情報(Content ID)と取扱方針(Usage Policy)をメッセージとして図7で説明したICV計算方法に従って計算される。なお、初期値は、IV=0としても、記録再生器暗号処理部302の内部メモリ307にチェック値A生成用初期値IV_aを保存しておき、それを使用してもよい。最後に、チェック値Aとヘッダ(Header)内に格納されたチェック値:ICV_aを比較し、一致していた場合にはステップS53へ進む。【0182】先に図4において説明したA、ICV_aは、識別情報、取扱方針の改竄を検証する

なされたコンテンツは、記録再生器2102、記録再生器2103と鍵ブロック4との間での認証が成立するので利用可能となる。【0176】上述のように、本発明のデータ处理装置においては、記録デバイスに複数の異なる鍵セットからなる鍵ブロックを構成し、一方、記録再生機器には、特定の鍵ブロックに対する認証可能なマスター鍵を格納する構成としたので、様々な利用態様に応じたコンテンツの利用制限を設定することが可能となる。【0177】なお、1つの能な鍵ブロックを複数、例えば1～kとし、他の記録再生器において指定可能な鍵ブロックをp～qのように複数とすることも可能であり、また、共通に利用可能な鍵ブロックを複数設ける構成としてもよい。【0178】(7)記録ダウンロード処理次に、本発明のデータ処理装置において、記録再生器400から記録デバイス400の外部メモリにコンテンツをダウンロードする処理について説明する。【0179】図22にデバイス400へコンテンツをダウンロードする手順を説明する流れ図である。なお、図22においては、既に記録再生器300と記録デバイス400との間で上述した相互認証処理が完了しているものとする。【0180】ステップS50の制御部301は、読み取り部304を使ってコンテンツを格納したメディア500から所定のフォーマットに従ったデータを読み出すか、通信部305を使って通信手段600から所定のフォーマットに従ってデータを受信する。そして、記録再生器300の制御部301は、データの内のヘッダ(Header)部分(図4参照)を記録再生器300の記録再生器暗号処理部302に送信する。【0181】次に、ステップS52において、ステップS51でヘッダ(Header)を受信した記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308にチェック値Aを計算させる。チェック値Aは、図23に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵K_ic_vaを鍵とし、識別情報(Content ID)と取扱方針(Usage Policy)をメッセージとして図7で説明したICV計算方法に従って計算される。なお、初期値は、IV=0としても、記録再生器暗号処理部302の内部メモリ307にチェック値A生成用初期値IV_aを保存しておき、それを使用してもよい。最後に、チェック値Aとヘッダ(Header)内に格納されたチェック値:ICV_aを比較し、一致していた場合にはステップS53へ進む。【0182】先に図4において説明したA、ICV_aは、識別情報、取扱方針の改竄を検証する

るためのチェック値である。記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵K_{icva}を鍵とし、識別情報(Content ID)と取扱方針(Usage Policy)をメッセージとして図7で説明したICV計算方法に従って計算されるチェック値Aが、ヘッダ(Header)内に格納されたチェック値:ICVaと一致した場合には、識別情報、取扱方針の改竄がないと判断される。

$$K_{dis} = DES(MK_{dis}, Content ID \wedge IV_{dis})$$

【0185】ここで、MK_{dis}は、配送鍵K_{dis}を生成するための配送鍵用マスター鍵であり、これは、前述したように記録再生器300の内部メモリに格納されている鍵である。またContent IDはコンテンツデータのヘッダ部の識別情報であり、さらにIV_{dis}は、配送鍵用初期値である。また、上記式において、DES()は、第1引数を暗号鍵として、第2引数の値を暗号化する関数であり、演算 \wedge は64ビット単位の排他的論理和を示す。【0186】ステップS54において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308を使って、ステップS53で生成した配送鍵K_{dis}を用いて、読み取り部304を介して受信したメディア500、または、通信部305を介して通信手段600から受信したデータのヘッダ部に格納されたブロック情報鍵K_{b1t}とコンテンツ鍵K_{con}(図4参照)の復号化処理を行う。図4に示されるようにこれらブロック情報鍵K_{b1t}とコンテンツ鍵K_{con}は、DVD、CD等のメディア、あるいはインターネット等の通信路上では、配送鍵K_{dis}によって予め暗号化処理が施されている。【0187】さらに、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308を使って、ステップS54で復号化したブロック情報鍵K_{b1t}でブロック情報(BIT)を復号化する。図4に示されるようにブロック情報(BIT)は、DVD、CD等のメディア、あるいはインターネット等の通信路上では、ブロック情報鍵K_{b1t}によって予め暗号化処理が施されている。【0188】さらに、ステップS56において、記録再生器暗号処理部302の制御部306は、ブロック情報鍵K_{b1t}、コンテンツ鍵K_{con}およびブロック情報(BIT)を8バイト単位に分割し、それら全てを排他的論理和する(加算、減算等、いずれの演算でもよい)。次に、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308にチェック値B(ICVb)を計算させる。チェック値Bは、図24に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵K_{icvb}を鍵とし、先ほど計算した排他的論

【0183】次に、ステップS53において、記録再生器暗号処理部302の制御部306は、配送鍵K_{dis}の生成を記録再生器暗号処理部302の暗号/復号化部308に行わせる。配送鍵K_{dis}の生成方法としては、例えば次のように生成する。【0184】【数4】

$$K_{dis} = DES(MK_{dis}, Content ID \wedge IV_{dis})$$

理和値をDESで暗号化して生成する。最後に、チェック値BとHeader内のICVbを比較し、一致していた場合にはステップS57へ進む。【0189】先に図4において説明したように、ICVbは、ブロック情報鍵K_{b1t}、コンテンツ鍵K_{con}、ブロック情報(BIT)の改竄を検証するためのチェック値である。記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵K_{icvb}を鍵とし、ブロック情報鍵K_{b1t}、コンテンツ鍵K_{con}およびブロック情報(BIT)を8バイト単位に分割し排他的論理和して得られる値をDESで暗号化して生成したチェック値Bが、ヘッダ(Header)内に格納されたチェック値:ICVbと一致した場合には、ブロック情報鍵K_{b1t}、コンテンツ鍵K_{con}、ブロック情報の改竄がないと判断される。【0190】ステップS58において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308に中間チェック値の計算をさせる。中間チェック値は、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されている総チェック値生成鍵K_{icvt}を鍵とし、検証したヘッダ(Header)内のチェック値A、チェック値B、保持しておいた全てのコンテンツチェック値をメッセージとして図7で説明したICV計算方法に従って計算する。なお、初期値IV=0としても、記録再生器暗号処理部302の内部メモリ307に総チェック値生成用初期値IVtを保存しておく、それを使用してもよい。また、生成した中間チェック値は、必要に応じて記録再生器300の記録再生器暗号処理部302に保持しておく。【0191】この中間チェック値は、チェック値A、チェック値B、全てのコンテンツチェック値をメッセージとして生成されるものであり、これらの各チェック値の検証対象となっているデータについての検証を中間チェック値の照合処理によって行なってもよい。しかし、本実施例においては、システム全体の共有データとしての非改竄性検証処理と、ダウンロード処理後に各記録再生機器300のみが占有する占有データとして識別するための検証処理を区別して実行可能とするために、中間チェック値からさらに複数の異なるチェック値、すなわち総チェック値ICVtと、記録再生器固有チェック値I

CV_{dev} とを別々に、中間チェック値に基づいて生成可能としている。これらのチェック値については後段で説明する。【0192】記録再生器暗号処理部302の制御部6は、記録再生器暗号処理部302の暗号／復号化部308に総チェック値 ICV_t の計算をさせる。総チェック値 ICV_t は、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているシステム署名鍵 K_{sys} を鍵とし、中間チェック値をDESで暗号化して生成する。最後に、生成した総チェック値 ICV_t とステップS51で保存しておいたHeader内の ICV_t を比較し、一致していた場合には、ステップS58へ進む。システム署名鍵 K_{sys} は、複数の記録再生器、すなわちある一定のデータの記録再生処理を実行するシステム集合全体において共通する署名鍵である。【0194】次に、ステップS58において記録再生器300の制御部301は、ブロック情報(BIT)内のコンテンツブロック情報を取り出し、コンテンツブロックが検証対象になっているかいないか調べる。コンテンツブロックが検証対象になっている場合には、ヘッダ中のブロック情報中にコンテンツチェック値が格納されている。【0195】コンテンツブロックが検証対象になっていた場合には、該当するコンテンツブロックを、記録再生器300の読み取り部304を使ってメディア500から読み出すか、記録再生器300の通信部305を使って通信手段600から受信し、記録再生器300の記録再生器暗号処理部302へ送信する。これを受信した記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308にコンテンツ中間値を計算させる。【0196】コンテンツ中間値は、暗号化したコンテンツ鍵 K_{con} で、入力されたコンテンツブロックをDESのCBCモードで復号化し、その結果を8バイトごとに区切り、全て排他的論理和(加算、減算等、いずれの演算でもよい)して生成する。【0197】記録再生器暗号処理部306は、記録再生器暗号処理部302の暗号／復号化部308にコンテンツチェック値の計算をさせる。コンテンツチェック値は、記録再生器暗号処理部302の内部メモリ307に保存されているコンテンツチェック値生成鍵 K_{icvc} を鍵とし、コンテンツ中間値をDES

Sで暗号化して生成する。そして、記録再生器暗号処理部302の制御部306は、当該コンテンツチェック値と、ステップS51で記録再生器300の制御部301から受信したコンテンツブロック内の ICV を比較し、その結果を記録再生器300の制御部301に渡す。これを受信した記録再生器300の制御部301は、検証に成功していた場合、次の検証対象コンテンツブロックを取り出して記録再生器300の記録再生器暗号処理部302に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理を繰り返す。なお、Header生成側と合わせておけば、 $IV=0$ としても、記録再生器暗号処理部302の内部メモリ307にコンテンツチェック値生成用初期値 IV_c を保存しておき、それを使【0198】用してもよい。また、チェックした全てのコンテンツチェック値は、記録再生器300の記録再生器暗号処理部302に保持しておく。さらにまた、記録再生器300の記録再生器暗号処理部302は、検証対象のコンテンツブロックの検証順序を監視し、順序が間違っていたり、同一のコンテンツブロックを2回以上検証させられたりした場合には、認証に失敗したものとする。そして、全ての検証が成功した場合には、ステップS59へ進む。【0199】次に、ステップS59において、記録再生器300の記録再生器暗号処理部302は、ステップS54で復号化しておいたブロック情報鍵 K_{bit} とコンテンツ鍵 K_{con} を、記録再生器暗号処理部302の暗号／復号化部308に、相互認証の際に共有しておいたセッション鍵 K_{ses} で暗号化させる。記録再生器300の制御部301は、セッション鍵 K_{ses} で暗号化されたブロック情報鍵 K_{bit} とコンテンツ鍵 K_{con} を記録再生器300の記録再生器暗号処理部302から読み出し、これらのデータを記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。【0200】次に、ステップS60において、記録再生器300から送信してきたブロック情報鍵 K_{bit} とコンテンツ鍵 K_{con} を受信した記録デバイス400は、受信したデータを記録デバイス暗号処理部401の暗号／復号化部406に、相互認証の際に共有しておいたセッション鍵 K_{ses} で復号化させ、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵 K_{str} で再暗号化させる。最後に、記録再生器300の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400から保存鍵 K_{str} で再暗号化されたブロック情報鍵 K_{bit} とコンテンツ鍵 K_{con} を読み出す。そして、これらの鍵を、配送鍵 K_{dis} で暗号化されたブロック情報鍵 K_{bit} とコンテンツ鍵 K_{con} に置き換える。【0201】ステップS61において、記録再生器300

0の制御部301は、データのヘッダ部の取扱方針(Usage Policy)から利用制限情報を取り出し、ダウンロードしたコンテンツが当該記録再生器300のみで利用できる(この場合、利用制限情報が1に設定)か、別の同様な記録再生器300でも利用できる(この場合、利用制限情報が0に設定)か判定する。判定の結果、利用制限情報が1であった場合には、ステップS62に進む。0の制御部301は、記録再生器固有のチェック値を記録再生器300の記録再生器暗号処理部302に計算させる。記録再生器固有のチェック値は、図25に示すように記録再生器暗号処理部302の内部メモリ307に保存されている記録再生器署名鍵Kdevを鍵とし、ステップS58で保持しておいた中間チェック値をDESで暗号化して生成する。計算された記録再生器固有のチェック値ICVdevは、総チェック値ICVtの代わりに上書きされる。【0202】先に説明したように、システィンは、配信システムに共通の署名またはICVをつけるために使用するシステム署名鍵であり、また、記録再生器署名鍵Kdevは、記録再生器毎に異なり、記録再生器が署名またはICVをつけるために使用する記録再生器署名鍵である。すなわち、システム署名鍵Ksysによって署名されたデータは、同じシステム署名鍵を有するシステム(記録再生器)によってチェックが成功、すなわち総チェック値ICVtが一致することになるので、共通に利用可能となるが、記録再生器署名鍵Kdevを用いて署名された場合には、記録再生器署名鍵はその記録再生器に固有の鍵であるので、記録再生器署名鍵Kdevを用いて署名されたデータ、すなわち、署名後、記録デバイスに格納されたデータは、他の記録再生器に、その記録デバイスを装着して再生しようとした場合、記録再生器固有のチェック値ICVdevが不一致となり、エラーとなるので再生できないことになる。【0204】0の制御部301は、コンテンツを記録デバイス400の外部メモリ402に保存する。【0205】図26は、記録デバイス内のコンテンツ状況を示す図である。図27は、利用制限情報が1の場合における記録デバイス内のコンテンツ状況を示す図である。図26が図4と異なる点は、コンテンツブロック情報鍵Kbitとコンテンツ鍵Kconが配信鍵Kdisで暗号化されているか、保存鍵Kstrで暗号化されているかだけである。また、図27が図26と異なる点は、中間チェック値から計算されるチェック値が、図26ではシステム署名鍵

Ksysで暗号化されているのに対し、図27では記録再生器固有の記録再生器署名鍵Kdevで暗号化されていることである。【0206】なお、図22の処理フローにおいて、ステップS52でチェック値Aの検証に失敗した場合、ステップS56でチェック値Bの検証に失敗した場合、ステップS57で総チェック値ICVtの検証に失敗した場合、ステップS58で各コンテンツブロックのコンテンツチェック値の検証に失敗した場合には、ステップS64に進み、所定のエラー表示を行う。【0207】また、ステップS63へ進む。【0208】(8) 記録デバイス格納情報の再生処理次に記録デバイス400の外部メモリ402に格納されたコンテンツ情報の記録再生器300での再生処理について説明する。【0209】図28は、記録再生器300が記録デバイス400からコンテンツを読み出し、コンテンツを利用システムする手順を説明する流れ図である。なお、図28においても、既に記録再生器300と記録デバイス400との間で相互認証が完了しているものとする。【0210】ステップS0の制御部301は、記録デバイスコントローラ303を使って記録デバイス400の外部メモリ402からコンテンツを読み出す。そして、記録再生器300の制御部301は、データの内のヘッダ(Header)部分を記録再生器300の記録再生器暗号処理部302に送信する。ステップS72は、「(7) 記録再生器から記録デバイスへのダウンロード処理」において説明したステップS52と同様の処理であり、ヘッダ(Header)を受信した記録再生器暗号処理部302の制御部306が、記録再生器暗号処理部302の暗号/復号化部308にチェック値Aを計算させる処理である。チェック値Aは、先に説明した図23に示すように記録再生器暗号処理部302の内部メモリ307に保存されているチェック値ICV生成鍵Kicvaを鍵とし、識別情報(Content ID)と取扱方針(Usage Policy)をメッセージとして図7で説明したと同様のICV計算方法に従って計算される。【0211】ステップS1aは、識別情報、取扱方針の改竄を検証するためのチェック値である。記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵Kicvaを鍵とし、識別情報(Content ID)と取扱方針(Usage Policy)をメッセージとして図7で説明したICV計算方法に従って計算されるチェック値Aが、ヘッダ(Header)内に格納されたチェック値:ICVaと一致した場合には、記録デバイス400に格納された識別情報、取扱方針の改竄はないと判断される。

【0212】次に、ステップS73において、記録再生器300の制御部301は、読み出したヘッダ(Header)部分からブロック情報鍵Kbitとコンテンツ鍵Kconを取り出し、記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。記録再生器300から送信されてきたブロック情報鍵Kbitとコンテンツ鍵Kconを受信した記録デバイス400は、受信したデータを記録デバイス暗号処理部401の暗号/復号化部406に、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵Kstrで復号化処理させ、相互認証の際に共有しておいたセッション鍵Ksesで再暗号化させる。そして、記録再生器300の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400からセッション鍵Ksesで再暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを読み出す。【0213】次に、ステップS74において、記録再生器300の制御部301は、受信したセッション鍵Ksesで再暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを記録再生器300の記録再生器暗号処理部302に送信する。【0214】セッション鍵Ksesロック情報鍵Kbitとコンテンツ鍵Kconを受信した記録再生器300の記録再生器暗号処理部302は、記録再生器暗号処理部302の暗号/復号化部308に、セッション鍵Ksesで暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを、相互認証の際に共有しておいたセッション鍵Ksesで復号化させる。そして、復号化したブロック情報鍵Kbitで、ステップS71で受信しておいたブロック情報を復号化する。【0215】なお、記録再生器300の記録再生器暗号処理部302は、復号化したブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報BITを、ステップS71で受信しておいたブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報BITに置き換えて保持しておく。また、記録再生器300の制御部301は、復号化されたブロック情報BITを記録再生器300の記録再生器暗号処理部302から読み出しておく。【0216】ステップS75は、「(7) 記録再生器300から記録デバイスへのダウンロード処理」において説明したステップS56と同様の処理である。記録再生器暗号処理部302の制御部306が、記録デバイス400から読み出したブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報(BIT)を8バイト単位に分割し、それら全てを排他的論理和する。次に、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308にチェック値B

(ICVb)を計算させる。チェック値Bは、先に説明した図24に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵Kicvbを鍵とし、先ほど計算した排他的論理和値をDESで暗号化して生成する。最後に、チェック値BとHeader内のICVbを比較し、一致していた場合にはステップS76へ進む。【0217】先に説明したように、チェック値Bは、ブロック情報鍵Kbit、コンテンツ鍵Kcon、ブロック情報の改竄を検証するためのチェック値である。記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵Kicvbを鍵とし、記録デバイス400から読み出したブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報(BIT)を8バイト単位に分割し排他的論理和して得られる値をDESで暗号化して生成したチェック値Bが、記録デバイス400から読み出したデータ中のヘッダ(Header)内に格納されたチェック値:ICVbと一致した場合には、記録デバイス400に格納されたデータのブロック情報鍵Kbit、コンテンツ鍵Kcon、ブロック情報の改竄はないと判断される。【0218】ステップS76で処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308に中間チェック値の計算をさせる。中間チェック値は、先に説明した図25に示すように記録再生器暗号処理部302の内部メモリ307に保存されている総チェック値生成鍵Kicvtを鍵とし、検証したヘッダ(Header)内のチェック値A、チェック値B、保持しておいた全てのコンテンツチェック値をメッセージとして図7他で説明したICV計算方法に従って計算する。なお、初期値はIV=0としても、記録再生器暗号処理部302の内部メモリ307に総チェック値生成用初期値にIVtを保存しておき、それを使用してもよい。また、生成した中間チェック値は、必要に応じて記録再生器300の記録再生器暗号処理部302に保持しておく。【0219】次に、ステップS77において、記録再生器300の制御部301は、記録デバイス400の外部メモリ402から読み出したデータのヘッダ部に含まれる取扱方針(Usage Policy)から利用制限情報を取り出し、ダウンロードしたコンテンツが当該記録再生器300のみで利用できる(利用制限情報が1)か、別の同様な記録再生器300でも利用できる(利用制限情報が0)か判定する。判定の結果、利用制限情報が1、すなわちダウンロードしたコンテンツが当該記録再生器300のみで利用できる利用制限が設定されている場合には、ステップS80に進み、利用制限情報が0、すなわち別の同様な記録再生器300でも利用できる設定であった場合には、ステップS78に進む。なお、ステップS77の処理は、暗号処理部302が行なってもよい。

【0220】ステップS78においては、(7)記録再生器から記録デバイスへのダウンロード処理において説明したステップS58と同様の総チェック値ICVtの計算が実行される。すなわち、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308に総チェック値ICVtの計算をさせる。総チェック値ICVtは、先に説明した図25に示すように記録再生器暗号処理部302の内部メモリ307に保存されているシステム署名鍵Ksyysを鍵とし、中間チェック値DESで暗号化して生成する。【0221】において生成した総チェック値ICVtとステップS71で保存しておいたヘッダ(Header)内のICVtを比較し、一致していた場合には、ステップS82へ進む。【0222】先に説明したように、総チェック値ICVtは、ICVa、ICVb、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成された総チェック値がヘッダ(Header)内に格納されたチェック値:ICVtと一致した場合には、記録デバイス400に格納されたデータにおいて、ICVa、ICVb、各コンテンツブロックのチェック値全ての改竄はないと判断される。【0223】ステップS77での判定において、ダウンロードしたコンテンツが当該記録再生器300のみで利用できる設定であった場合、すなわち設定情報が1であった場合は、ステップS80に進む。【0224】ステップS処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308に、記録再生器固有のチェック値ICVdevの計算をさせる。記録再生器固有のチェック値ICVdevは、先に説明した図25に示すように記録再生器暗号処理部302の内部メモリ307に保存されている記録再生器固有の記録再生器署名鍵Kdevを鍵とし、中間チェック値DESで暗号化して生成する。ステップS81において、ステップS80で計算した記録再生器固有のチェック値ICVdevとステップS71で保存しておいたHeader内のICVdevを比較し、一致していた場合には、ステップS82へ進む。【0225】このように、システム署名鍵Ksyysって署名されたデータは、同じシステム署名鍵を有するシステム(記録再生器)によってチェックが成功、すなわち総チェック値ICVtが一致することになるので共通に利用可能となり、記録再生器署名鍵Kdevを用いて署名された場合には、記録再生器署名鍵はその記録再生器に固有の鍵であるので、記録再生器署名鍵Kdevを用いて署名されたデータ、すなわち、署名後、記録デバイスに格納されたデータは、他の記録再生器に、その

記録デバイスを装着して再生しようとした場合、記録再生器固有のチェック値ICVdevが不一致となり、エラーとなるので再生できないことになる。従って、利用制限情報の設定によって、システムに共通に使用できるコンテンツ、記録再生器固有に利用できるコンテンツを自在に設定することが可能となる。【0226】ステップS82に0の制御部301は、ステップS74で読み出しておいたブロック情報BIT内のコンテンツブロック情報を取り出し、コンテンツブロックが暗号化対象になっているかいないか調べる。暗号化対象になっていた場合には、該当するコンテンツブロックを、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400の外部メモリ402から読み出し、記録再生器300の記録再生器暗号処理部302へ送信する。これを受信した記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308にコンテンツを復号化するとともに、コンテンツブロックが検証対象になっている場合には次のステップS83においてコンテンツチェック値を検証させる。【0227】ステップS82「記録デバイスへのダウンロード処理」において説明したステップS58と同様の処理である。記録再生器300の制御部301は、ブロック情報(BIT)内のコンテンツブロック情報を取り出し、コンテンツブロックが検証対象になっているかいないかをコンテンツチェック値の格納状況から判定し、コンテンツブロックが検証対象になっていた場合には、該当するコンテンツブロックを、記録デバイス400の外部メモリ402から受信し、記録再生器300の記録再生器暗号処理部302へ送信する。これを受信した記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308にコンテンツ中間値を計算させる。【0228】号化したコンテンツ鍵Kconで、入力されたコンテンツブロックをDESのCBCモードで復号化し、その結果を8バイトに区切り全て排他的論理和して生成する。【0229】部306は、記録再生器暗号処理部302の暗号/復号化部308にコンテンツチェック値の計算をさせる。この結果によって、記録再生器暗号処理部302の内部メモリ307に保存されているコンテンツチェック値生成鍵Kicvcを鍵とし、コンテンツ中間値をDESで暗号化して生成する。そして、記録再生器暗号処理部302の制御部306は、当該コンテンツチェック値と、ステップS71で記録再生器300の制御部301から受信したコンテンツブロック内のICVを比較し、その結果を記録再生器300の制御部301に渡す。これを受信した記録再生器300の制御部301は、検証に成功していた場合、次の検証対象コンテンツブロック

を取り出して記録再生器300の記録再生器暗号処理部302に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理を繰り返す。なお、初期値はIV=0としても、記録再生器暗号処理部302の内部メモリ307にコンテンツチェック値生成用初期値IVcを保存しておき、それを使用してもよい。また、チェックした全てのコンテンツチェック値は、記録再生器300の記録再生器暗号処理部302に保持しておく。さらによると、記録再生器300の記録再生器暗号処理部302は、検証対象のコンテンツブロックの検証順序を監視し、順序が間違っていたり、同一のコンテンツブロックを2回以上検証させられたりした場合には、認証に失敗したものとする。【0230】記録再生器300の制御部303にコンテンツチェック値の比較結果(検証対象になっていない場合、比較結果は全て成功とする)を受信し、検証に成功していた場合には、記録再生器300の記録再生器暗号処理部302から復号化されたコンテンツを取り出す。そして、次の復号化対象コンテンツブロックを取り出して記録再生器300の記録再生器暗号処理部302に復号化させ、全てのコンテンツブロックを復号化するまで繰り返す。【0231】なお、ステップS83において記録再生器300の記録再生器暗号処理部302は、コンテンツチェック値の検証処理において不一致となった場合には、検証失敗としてその時点で処理を中止し、残るコンテンツの復号化は行わない。また、記録再生器300の記録再生器暗号処理部302は、復号化対象のコンテンツブロックの復号化順序を監視し、順序が間違っていたり、同一のコンテンツブロックを2回以上復号化させられたりした場合には、復号化に失敗したものとする。【0232】検証に失敗した場合、ステップS75でチェック値Bの検証に失敗した場合、ステップS79で総チェック値ICVtの検証に失敗した場合、ステップS81で記録再生器固有のチェック値ICVdeの検証に失敗した場合には、ステップS83で各コンテンツブロックのコンテンツチェック値の検証に失敗した場合、ステップS84に進み、所定のエラー表示を行う。【0233】以上説明してウンドロードしたり、利用したりする際に、重要なデータやコンテンツを暗号化しておいて隠蔽化したり、改竄検証ができるだけでなく、ブロック情報BITを復号化するためのブロック情報鍵Kbit、コンテンツを復号化するためのコンテンツ鍵Kconが記録デバイス固有の保存鍵Kstrで保存されているため、単純に記録メディア上のデータを別の記録メディアに複製したとしても、コンテンツを正しく復号化することができなくなることができる。より具体的には、例えば図28のステップS74において、記録デバイス毎に異なる保存鍵Ks

tで暗号化されたデータを復号化するため、別の記録デバイスではデータを正しく復号化できない構成を持つからである。【0234】(9) 相互認証後の鍵交換処理本発明の記録再生器300と記録デバイス400との間で実行される相互認証処理の後においてのみ、記録デバイスの利用を可能とし、また、その利用態様を制限した点がある。【0235】例えば、不正な複製等によってコンテンツを格納したメモリカード等の記録デバイスを生成し、これを記録再生器にセットして利用されることを排除するために、記録再生器300と、記録デバイス400間での相互認証処理を実行し、かつ認証OKとなったことを条件として、コンテンツ(暗号化された)の記録再生器303および記録デバイス400間での転送を可能としている。【0236】上記の制限的処理を実現するために、本発明のデータ処理装置においては、記録デバイス400の暗号処理部401での処理は、すべて、予め設定されたコマンド列に基づいて実行される構成となっている。すなわち、記録デバイスは、コマンド番号に基づくコマンドを順次レジスタから取り出して実行するコマンド処理構成を持つ。この記録デバイスでのコマンド処理構成を説明する図を図29に示す。【0237】図29に示すように記録再生器302を有する記録再生器300と記録デバイス暗号処理部401を有する記録デバイス400間においては、記録再生器300の制御部301の制御のもとに記録デバイスコントローラ303から記録デバイス400の通信部(受信レジスタを含む)404に対してコマンド番号(No.)が出力される。【0238】記録デバイス400は、周囲の制御部403にコマンド番号管理部2201を有する。コマンド番号管理部2201は、コマンドレジスタ2902を保持しており、記録再生器300から出力されるコマンド番号に対応するコマンド列を格納している。コマンド列は、図29の右に示すようにコマンド番号0からyまで順次、コマンド番号に対して実行コマンドが対応付けられている。コマンド番号管理部2201は、記録再生器300から出力されるコマンド番号を監視し、対応するコマンドをコマンドレジスタ2902から取り出して実行する。【0239】コマンドレジスタ2902にコマンドシーケンスは、図29の右に示すように、認証処理シーケンスに関するコマンド列が先行するコマンド番号0～kに対応付けられている。さらに、認証処理シーケンスに関するコマンド列の後のコマンド番号p～sに復号、鍵交換、暗号処理コマンドシーケンス1、さらに、後続するコマンド番号u～yに復号、鍵交換、暗号

処理コマンドシーケンス2が対応付けされている。【0240】`on`を記録デバイスが受信する処理であり、その後、前述の図29で示したコマンド列`p~s`が開始される。コマンド列`p~s`は認証処理コマンド`0~k`が完了し、図29に示す認証フラグ`2903, 2904`に認証済みのフラグがセットされた後開始される。これは、コマンド番号管理部`2901`がコマンド番号を`0`から昇順でのみ受け付けることによって保証される。【0248】ステップ`記録再生器`から受信したセッション鍵`Kses`で暗号化されたデータ（e.g. ブロック情報鍵`Kbit`, コンテンツ鍵`Kcon`）をレジスタに格納する処理である。【0249】`es`で暗号化されたデータ（e.g. ブロック情報鍵`Kbit`, コンテンツ鍵`Kcon`）をレジスタから取り出してセッション鍵`Kses`で復号する処理を実行するステップである。【0250】ステップ`S3004`は、セッション鍵`Kses`で復号化されたデータ（e.g. ブロック情報鍵`Kbit`, コンテンツ鍵`Kcon`）を保存鍵`Kstr`で暗号化する処理を実行するステップである。【0251】上記の処理とは、先の図29で説明したコマンドレジスタ中のコマンド番号`p~s`に含まれる処理である。これらの処理は、記録デバイス`400`のコマンド番号管理部`2901`において記録再生器`300`から受信するコマンド番号`p~s`に従って記録デバイス暗号処理部`401`が順次実行する。【0252】次のステップ`S3005`は、保存鍵`Kstr`で暗号化したデータ（e.g. ブロック情報鍵`Kbit`, コンテンツ鍵`Kcon`）を記録デバイスの外部メモリに格納するステップである。このステップにおいては、記録デバイス暗号処理部`401`から記録再生器`300`が保存鍵`Kstr`で暗号化したデータを読み出して、その後に記録デバイス`400`の外部メモリ`402`に格納してもよい。【0253】上述のステップ`S3002~S3004`の具体例を図30, 31を用いて説明する。【0246】図29に示すコマンドシーケンスは、認証処理を先行して処理するようにコマンド番号が付与されており、その後の処理に復号、鍵交換、暗号化処理の処理シーケンスが格納されている。【0245】復号、鍵交換、暗号化処理の実行シーケンスの実行順序は、コマンド番号`p~s`に設定された昇順の順序で実行される。【0247】図30において記録再生器`300`からセッション鍵`Kses`で暗号化されたデータ（e.g. ブロック情報鍵`Kbit`, コンテンツ鍵`Kcon`）を記録デバイス`400`が受信する処理である。【0248】`es`で暗号化されたデータ（e.g. ブロック情報鍵`Kbit`, コンテンツ鍵`Kcon`）をレジスタに格納する処理である。【0249】`es`で暗号化されたデータ（e.g. ブロック情報鍵`Kbit`, コンテンツ鍵`Kcon`）をレジスタから取り出してセッション鍵`Kses`で復号する処理を実行するステップである。【0250】ステップ`S3004`は、セッション鍵`Kses`で復号化されたデータ（e.g. ブロック情報鍵`Kbit`, コンテンツ鍵`Kcon`）を保存鍵`Kstr`で暗号化する処理を実行するステップである。【0251】上記の処理とは、先の図29で説明したコマンドレジスタ中のコマンド番号`p~s`に含まれる処理である。これらの処理は、記録デバイス`400`のコマンド番号管理部`2901`において記録再生器`300`から受信するコマンド番号`p~s`に従って記録デバイス暗号処理部`401`が順次実行する。【0252】次のステップ`S3005`は、保存鍵`Kstr`で暗号化したデータ（e.g. ブロック情報鍵`Kbit`, コンテンツ鍵`Kcon`）を記録デバイスの外部メモリに格納するステップである。このステップにおいては、記録デバイス暗号処理部`401`から記録再生器`300`が保存鍵`Kstr`で暗号化したデータを読み出して、その後に記録デバイス`400`の外部メモリ`402`に格納してもよい。【0253】上述のステップ`S3002~S3004`の実行順序は、連続して実行される割込み不可能な実行シーケンスであり、たとえば、ステップ`S3003`の復号処理終了時点で、記録再生器`300`からのデータ読み出し命令があったとしても、その読み出しコマンドは、コマンドレジスタ`2902`のコマンド番号`p~s`に設定された昇順の順序で実行される。【0254】図31は、先に図28において説明したように、記録デバイス`400`からコンテンツを読み出して記録再生器`300`において再生するコンテンツ再生処理において

記録デバイス`400`が受信する処理であり、その後、前述の図29で示したコマンド列`p~s`が開始される。コマンド列`p~s`は認証処理コマンド`0~k`が完了し、図29に示す認証フラグ`2903, 2904`に認証済みのフラグがセットされた後開始される。これは、コマンド番号管理部`2901`がコマンド番号を`0`から昇順でのみ受け付けることによって保証される。【0248】ステップ`記録再生器`から受信したセッション鍵`Kses`で暗号化されたデータ（e.g. ブロック情報鍵`Kbit`, コンテンツ鍵`Kcon`）をレジスタに格納する処理である。【0249】`es`で暗号化されたデータ（e.g. ブロック情報鍵`Kbit`, コンテンツ鍵`Kcon`）をレジスタから取り出してセッション鍵`Kses`で復号する処理を実行するステップである。【0250】ステップ`S3004`は、セッション鍵`Kses`で復号化されたデータ（e.g. ブロック情報鍵`Kbit`, コンテンツ鍵`Kcon`）を保存鍵`Kstr`で暗号化する処理を実行するステップである。【0251】上記の処理とは、先の図29で説明したコマンドレジスタ中のコマンド番号`p~s`に含まれる処理である。これらの処理は、記録デバイス`400`のコマンド番号管理部`2901`において記録再生器`300`から受信するコマンド番号`p~s`に従って記録デバイス暗号処理部`401`が順次実行する。【0252】次のステップ`S3005`は、保存鍵`Kstr`で暗号化したデータ（e.g. ブロック情報鍵`Kbit`, コンテンツ鍵`Kcon`）を記録デバイスの外部メモリに格納するステップである。このステップにおいては、記録デバイス暗号処理部`401`から記録再生器`300`が保存鍵`Kstr`で暗号化したデータを読み出して、その後に記録デバイス`400`の外部メモリ`402`に格納してもよい。【0253】上述のステップ`S3002~S3004`の実行順序は、連続して実行される割込み不可能な実行シーケンスであり、たとえば、ステップ`S3003`の復号処理終了時点で、記録再生器`300`からのデータ読み出し命令があったとしても、その読み出しコマンドは、コマンドレジスタ`2902`のコマンド番号`p~s`に設定された昇順の順序で実行される。【0254】図31は、先に図28において説明したように、記録デバイス`400`からコンテンツを読み出して記録再生器`300`において再生するコンテンツ再生処理において

実行される処理の一部を構成するものである。具体的には図28におけるステップS73において実行される処理である。【0255】図31において、ステップS3101は記録デバイス400の外部メモリ402から保存鍵Kstrで暗号化されたデータ（e.g. ブロック情報鍵Kbit、コンテンツ鍵Kcon）の読み出しを実行するステップである。【0256】ステップS3102は、記録デバイス400の外部メモリから読み出した保存鍵Kstrで暗号化されたデータ（e.g. ブロック情報鍵Kbit、コンテンツ鍵Kcon）をレジスタに格納するステップである。このステップにおいては、記録デバイス400の外部メモリ402から記録再生器300が保存鍵Kstrで暗号化したデータを読み出して、その後に記録デバイス400のレジスタに格納してもよい。【0257】ステップS3103は、暗号化されたデータ（e.g. ブロック情報鍵Kbit、コンテンツ鍵Kcon）をレジスタから取り出して保存鍵Kstrで復号処理するステップである。【0258】ステップS3104は、復号化されたデータ（e.g. ブロック情報鍵Kbit、コンテンツ鍵Kcon）をセッション鍵Ksesで暗号化処理するステップである。【0259】上記の処理ステップは、先の図29で説明したコマンドレジスタ中のコマンド番号u～yに含まれる処理である。これらの処理は、記録デバイスのコマンド番号管理部2901において記録再生器300から受信するコマンド番号u～yに従って記録デバイス暗号処理部406が順次実行する。【0260】ステップS3105は、Ksesで暗号化したデータ（e.g. ブロック情報鍵Kbit、コンテンツ鍵Kcon）を記録デバイスから記録再生器へ送信する処理である。【0261】上述のステップは、連続して実行される割込み不可能な実行シーケンスであり、たとえば、ステップS3103の復号処理終了時点では、記録再生器300からのデータ読み出し命令があったとしても、その読み出しコマンドは、コマンドレジスタ2902のコマンド番号u～yに設定された昇順のコマンド番号とは異なるため、コマンド番号管理部2901は、読み出しの実行を受け付けない。従って、記録デバイス400における鍵交換の際に発生する復号データを外部、例えば記録再生器300から読み出すことは不可能となり、鍵データあるいはコンテンツの不正な読み出しを防止できる。【0262】なお、図30、31に示したコマンドレジスタ2902に格

納されたコマンドシーケンスには、コンテンツ自体の鍵交換を伴う復号、暗号化処理を含ませてもよく、鍵交換によって復号、暗号化される対象は上述の例に限定されるものではない。【0263】以上、本発明のデータ処理装置における鍵交換処理について説明した。このように、本発明のデータ処理装置における鍵交換処理は、記録再生器と記録デバイス間での認証処理が終了した後においてのみ実行可能となり、さらに、鍵交換処理における復号データの外部からのアクセスが防止可能な構成となっているので、コンテンツ、鍵データの高度なセキュリティが確保される。【0264】（10）複数のコンテンツデータセットと、各フォーマットに対応するダウンロードおよび再生処理上述した実施例では、例えば図3に示すメディア500あるいは通信手段600におけるデータフォーマットが図4に示す1つの種類である場合について説明してきた。しかしながら、メディア500あるいは、通信手段600におけるデータフォーマットは、上述の図4に示すフォーマットに限らず、コンテンツが音楽である場合、画像データである場合、ゲーム等のプログラムである場合等、コンテンツに応じたデータフォーマットを採用することが望ましい。以下、複数の異なるデータデータフォーマットと、各フォーマットに対応する記録デバイスへのダウンロード処理および記録デバイスからの再生処理について説明する。【0265】図32～35に4つの異なるデータフォーマットを示す。各図の左側には、図3に示すメディア500、または通信手段600上におけるデータフォーマットを、また各図の右側には記録デバイス400の外部メモリ402に格納される場合のデータフォーマットを示してある。先に、図32～35に示すデータフォーマットの概略を説明し、その後、各フォーマットにおける各データの内容、および各フォーマットにおけるデータの差異について説明する。【0266】図32は、フォーマット0の概略を示す。このフォーマット0の特徴は、データ全体を任意の大きさのN個のデータブロック、すなわちブロック1～ブロックNに分割し、各ブロックについて任意に暗号化し、暗号化ブロックと非暗号化ブロック、すなわち平文ブロックを混在させてデータを構成できる点である。ブロックの暗号化は、コンテンツ鍵Kconによって実行されており、コンテンツ鍵Kconは、メディア上では配送鍵Kdisによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵Kstrによって暗号化される。ブロック情報鍵Kbitについてもメディア上では配送鍵Kdisによって暗号化され、記録デバイスにおける保存時

には、記録デバイスの内部メモリに格納された保存鍵K_{s t r}によって暗号化される。これらの鍵交換は、前述の「(9) 相互認証後の鍵交換処理」において説明した処理にしたがって実行される。【0267】図33は、フォーマットタイプ1は、フォーマットタイプ0と同様、データ全体をN個のデータブロック、すなわちブロック1～ブロックNに分割しているが、N個の各ブロックの大きさを同じ大きさとした点で前述のフォーマットタイプ0と異なる。コンテンツ鍵K_{c o n}によるブロックの暗号化処理態様は前述のフォーマットタイプ0と同様である。また、メディア上で配送鍵K_{d i s}によって暗号化され、記録デバイスにおける保存時には記録デバイスの内部メモリに格納された保存鍵K_{s t r}によって暗号化されるコンテンツ鍵K_{c o n}およびブロック情報鍵K_{b i t}構成も上述のフォーマットタイプ0と同様である。フォーマットタイプ1は、フォーマットタイプ0と異なり、固定的なブロック構成としたことで、ブロック毎のデータ長等の構成データが簡略化されるので、フォーマットタイプ0に比較してブロック情報のメモリサイズを減らすことが可能となる。【0268】図33の構成コンテンツが記録再生器固有に利用可能か否かを決定するフラグであるローカリゼーション・フラグ、さらに、コンテンツのコピー、ムーブ処理に関する許可フラグ、さらに、コンテンツ暗号化アルゴリズム、モード等、コンテンツに関する各種の利用制限情報および処理情報を格納する。【0273】チェック値A: I C V aは、識別情報、取扱方針に対するチェック値であり、例えば、前述の図23で説明した手法によって生成される。【0274】ブロック情報を暗号化するための鍵であり、先に説明したように、メディア上では配送鍵K_{d i s}によって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵K_{s t r}によって暗号化される。【0275】号化に用いる鍵であり、フォーマットタイプ0, 1では、ブロック情報鍵K_{b i t}と同様にメディア上では配送鍵K_{d i s}によって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵K_{s t r}によって暗号化される。なお、フォーマットタイプ2では、コンテンツ鍵K_{c o n}は、コンテンツ各ブロックに構成されるブロック鍵K_{b l c}の暗号化にも利用される。また、フォーマット・タイプ3においては、コンテンツ鍵K_{c o n}は存在しない。【0276】ブロック記述するテーブルであり、ブロックの大きさ、暗号化されているか否かについてのフラグ、すなわち各ブロックがチェックの対象(I C V)と、なっているか否かを示す情報を格納される。ブロックがチェックの対象となつ

について、それぞれ個別のブロック鍵K_{b l c}で暗号化されていること、さらに、コンテンツ鍵を用いず、各ブロック鍵K_{b l c}の暗号化は、メディア上では配送鍵K_{d i s}によって暗号化され、記録デバイス上では保存鍵K_{s t r}によって暗号化されている点である。コンテンツ鍵K_{c o n}は、メディア上、デバイス上、いずれにも存在しない。ブロック情報鍵K_{b i t}はメディア上では配送鍵K_{d i s}によって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵K_{s t r}によって暗号化される。【0271】次に、上記一タの内容について説明する。データは先に説明したように、ヘッダ部とコンテンツ部に大きく2つに分類され、ヘッダ部にはコンテンツ識別子、取扱方針、チェック値A, B, 総チェック値、ブロック情報鍵、コンテンツ鍵、ブロック情報が含まれる。【0272】取扱方針には、コンダ長、フォーマットタイプ(以下説明するフォーマット0～3)、例えばプログラムであるか、データであるか等のコンテンツタイプ、前述のコンテンツの記録デバイスへのダウンロード、再生の欄で説明したように、コンテンツが記録再生器固有に利用可能か否かを決定するフラグであるローカリゼーション・フラグ、さらに、コンテンツのコピー、ムーブ処理に関する許可フラグ、さらに、コンテンツ暗号化アルゴリズム、モード等、コンテンツに関する各種の利用制限情報および処理情報を格納する。【0273】チェック値A: I C V aは、識別情報、取扱方針に対するチェック値であり、例えば、前述の図23で説明した手法によって生成される。【0274】ブロック情報を暗号化するための鍵であり、先に説明したように、メディア上では配送鍵K_{d i s}によって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵K_{s t r}によって暗号化される。【0275】号化に用いる鍵であり、フォーマットタイプ0, 1では、ブロック情報鍵K_{b i t}と同様にメディア上では配送鍵K_{d i s}によって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵K_{s t r}によって暗号化される。なお、フォーマットタイプ2では、コンテンツ鍵K_{c o n}は、コンテンツ各ブロックに構成されるブロック鍵K_{b l c}の暗号化にも利用される。また、フォーマット・タイプ3においては、コンテンツ鍵K_{c o n}は存在しない。【0276】ブロック記述するテーブルであり、ブロックの大きさ、暗号化されているか否かについてのフラグ、すなわち各ブロックがチェックの対象(I C V)と、なっているか否かを示す情報を格納される。ブロックがチェックの対象となつ

ている場合は、ブロックのチェック値 ICV_i (ブロック i のチェック値) がテーブル中に定義されて格納される。このブロック情報は、ブロック情報暗号鍵 K_{bit} によって暗号化される。【0277】なお、ブロックのコンテンツチェック値 ICV_i は、ブロックが暗号化されている場合、平文 (復号文) 全体を 8 バイト単位で排他論理和した値を記録再生器 300 の内部メモリ 307 に格納されたコンテンツチェック値生成鍵 K_{icvc} で暗号化した値として生成される。また、ブロックが暗号化されていない場合は、ブロックデータ (平文) の全体を 8 バイト単位で図 36 に示す改竄チェック値生成関数 (DES-CBC-MAC、コンテンツチェック値生成鍵 K_{icvc} を鍵とする) に入力して得た値として生成される。図 36 にコンテンツブロックのチェック値 ICV_i を生成する構成例を示す。メッセージ M の各々が復号文データまたは平文データの各 8 バイトを構成する。【0278】は、ブロック内のパートのうち少なくとも 1 つがチェック値 ICV_i の対象データ、すなわち要チェックパートである場合は、そのブロックに関してコンテンツチェック値 ICV_i が定義される。ブロック i におけるパート j のチェック値 $P-ICV_{ij}$ は、パート j が暗号化されている場合、平文 (復号文) 全体を 8 バイト単位で排他論理和した値をコンテンツチェック値生成鍵 K_{icvc} で暗号化した値として生成される。また、パート j が暗号化されていない場合は、パートのブロックのデータ (平文) の全体を 8 バイト単位で図 36 に示す改竄チェック値生成関数 (DES-CBC-MAC、コンテンツチェック値生成鍵 K_{icvc} を鍵とする) に入力して得た値として生成される。【0279】さらに、1 つのブロック対象であることを示す [ICV フラグ = sub ject of ICV] であるパート、すなわち要チェックパートが 1 つのみ存在する場合は、上述の手法で生成したチェック値 $P-ICV_{ij}$ をそのままブロックのチェック値 ICV_i とし、また、1 つのブロック i 内にチェック対象であることを示す [ICV フラグ = sub ject of ICV] であるパートが複数存在する場合は、複数のパートチェック値 $P-ICV_{ij}$ をパート番号順に連結したデータを対象にして 8 バイト単位で図 37 に示す改竄チェック値生成関数 (DES-CBC-MAC、コンテンツチェック値生成鍵 K_{icvc} を鍵とする) に入力して得た値として生成される。図 37 にコンテンツブロックのコンテンツチェック値 ICV_i を生成する構成例を示す。【0280】なお、フォーマット・タイプでは、ブロックのチェック値 ICV_i は定義されない。【0281】チェック値 $B: ICV_b$ は、ブロック情報鍵、コンテンツ鍵、ブロック情報全体に対するチェック

値であり、例えば、前述の図 24 で説明した手法によって生成される。【0282】総チェック値 ICV_t は、前述のチェック値 $A: ICVa$ 、チェック値 $B: ICVb$ 、さらにコンテンツのチェック対象となっている各ブロックに含まれるチェック値 $ICVi$ 全体に対するチェック値であり、前述の図 25 で説明したようにチェック値 $A: ICVa$ 等の各チェック値から生成される中間チェック値にシステム署名鍵 $Ksys$ を適用して暗号化処理を実行することによって生成される。【0283】なお、フォーマット・タイプでは、総チェック値 ICV_t は、前述のチェック値 $A: ICVa$ 、チェック値 $B: ICVb$ にコンテンツデータ、すなわちブロック 1 のブロック鍵から最終ブロックまでのコンテンツデータ全体を連結したデータから生成される中間チェック値にシステム署名鍵 $Ksys$ を適用して暗号化処理を実行することによって生成される。【0284】にフォーマット・タイプ 2, 3 における総チェック値 ICV_t を生成する構成例を示す。【0285】固有チェック値 ICV_t が 1 にセットされている場合、すなわち、コンテンツが記録再生器固有に利用可能であることを示している場合に、総チェック値 ICV_t に置き換えるチェック値であり、フォーマット・タイプ 0, 1 の場合は、前述のチェック値 $A: ICVa$ 、チェック値 $B: ICVb$ 、さらにコンテンツのチェック対象となっている各ブロックに含まれるチェック値 $ICVi$ 全体に対するチェック値として生成される。具体的には、前述の図 25、または図 38 で説明したようにチェック値 $A: ICVa$ 等の各チェック値から生成される中間チェック値に記録再生器署名鍵 $Kdev$ を適用して暗号化処理を実行することによって生成される。【0286】次に記録再生器 300 から記録デバイス 400 に対するコンテンツのダウンロード処理、および記録再生器 300 における記録デバイス 400 からの再生処理について図 39~44 のフローを用いて説明する。【0287】まず、フォーマットのダウンロード処理について図 39 を用いて説明する。【0288】図 39 に示す処理は、例えば図 3 に示す記録再生器 300 に記録デバイス 400 を装着することによって開始される。ステップ S101 は、記録再生器と記録デバイス間における認証処理ステップであり、先に説明した図 20 の認証処理フローに従って実行される。【0289】認証フラグがセットされると、記録再生器 300 は、ステップ S102 において、例えばコンテンツデータを格納したメディア 500 から、読み取り部 304 を介して所定のフォーマットに従ったデータを読み出すか、通信部

【0281】チェック値 $B: ICV_b$ は、ブロック情報

305を使って通信手段600から所定のフォーマットに従ってデータを受信し、記録再生器300の制御部301が、データの内のヘッダ(Header)部分を記録再生器300の記録再生器暗号処理部302に送信する。【0289】記録再生器暗号処理部302の制御部306が記録再生器暗号処理部302の暗号/復号化部308にチェック値Aを計算させる。チェック値Aは、図23に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵K_{icva}を鍵とし、識別情報(Content ID)と取扱方針(Usage Policy)をメッセージとして図7を用いて説明したICV計算方法に従って計算される。次に、ステップS104において、チェック値Aとヘッダ(Header)内に格納されたチェック値:ICVaを比較し、一致していた場合にはステップS105へ進む。【0290】先に説明したようにチェック値A, aは、識別情報、取扱方針の改竄を検証するためのチェック値である。記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵K_{icva}を鍵とし、識別情報(Content ID)と取扱方針(Usage Policy)をメッセージとして、例えばICV計算方法に従って計算されるチェック値Aが、ヘッダ(Header)内に格納されたチェック値:ICVaと一致した場合には、識別情報、取扱方針の改竄がないと判断される。【0291】記録再生器暗号処理部302の制御部306は、配送鍵K_{dis}の取り出しあり生成を記録再生器暗号処理部302の暗号/復号化部308に行わせる。配送鍵K_{dis}の生成方法は、先に説明した図22のステップS53と同様、例えば配送鍵用マスター鍵MK_{dis}を用いて行われる。【0292】次にステップS106において、記録再生器暗号処理部302の制御部306が、記録再生器暗号処理部302の暗号/復号化部308を使って、生成した配送鍵K_{dis}を用いて、読み取り部304を介して受信したメディア500、または、通信部305を介して通信手段600から受信したデータのヘッダ部に格納されたブロック情報鍵K_{b1t}とコンテンツ鍵K_{con}の復号化を行う。【0293】さらに、ステップS107において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308において、復号化したブロック情報鍵K_{b1t}でブロック情報を復号化する。【0294】さらに、ステップS108において、記録再生器暗号処理部302の制御部306は、ブロック情報鍵K_{b1t}、コンテンツ鍵K_{con}およびブロック情報(BIT)から、チェック値B(ICVb')を生成する。チェック値Bは、図24に示すように、記録再生

器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵K_{icvb}を鍵とし、ブロック情報鍵K_{b1t}、コンテンツ鍵K_{con}およびブロック情報(BIT)からなる排他的論理和値をDESで暗号化して生成する。次に、ステップS109において、チェック値Bとヘッダ(Header)内のICVbを比較し、一致していた場合にはステップS110へ進む。【0295】先に説明したように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵K_{icvb}を鍵とし、ブロック情報鍵K_{b1t}、コンテンツ鍵K_{con}およびブロック情報(BIT)を8バイト単位に分割し排他的論理和して得られる値をDESで暗号化して生成したチェック値Bが、ヘッダ(Header)内に格納されたチェック値:ICVbと一致した場合には、ブロック情報鍵K_{b1t}、コンテンツ鍵K_{con}、ブロック情報の改竄がないと判断される。【0296】ステップS110において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308に中間チェック値の計算をさせる。中間チェック値は、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されている総チェック値生成鍵K_{icvt}を鍵とし、検証したHeader内のチェック値A、チェック値B、保持しておいた全てのコンテンツチェック値をメッセージとして図7他で説明したICV計算方法に従って計算する。なお、生成した中間チェック値は、必要に応じて記録再生器300の記録再生器暗号処理部302に保持しておく。【0297】次に、ステップS111において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308に総チェック値ICVt'の計算をさせる。総チェック値ICVt'は、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているシステム署名鍵K_{sys}を鍵とし、中間チェック値をDESで暗号化して生成する。次に、ステップS112において、生成した総チェック値ICVt'をヘッダ(Header)内のICVtを比較し、一致していた場合には、ステップS113へ進む。【0298】先に図4において説明したように、総チェック値ICVt'は、ICVa、ICVb、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成された総チェック値がヘッダ(Header)内に格納されたチェック値:ICVtと一致した場合には、ICVa、ICVb、各コンテンツブロックのチェック値全ての改竄がないと判断される。

【0299】次に、ステップS113において、記録再生器300の制御部301は、ブロック情報(BIT)内のコンテンツブロック情報を取り出し、コンテンツブロックが検証対象になっているかいないか調べる。コンテンツブロックが検証対象になっている場合には、ヘッダ中のブロック情報中にコンテンツチェック値が格納されている。【0300】コンテンツブロックが検証対象になつた場合には、ステップS114において、該当するコンテンツブロックを、記録再生器300の読み取り部304を使ってメディア500から読み出すか、記録再生器300の通信部305を使って通信手段600から受信し、記録再生器300の記録再生器暗号処理部302へ送信する。これを受信した記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308にコンテンツチェック値ICVi'を計算させる。【0301】コンテンツチェック値ICVi'を説明したようにブロックが暗号化されている場合、コンテンツ鍵Kconで、入力されたコンテンツブロックをDESのCBCモードで復号化し、その結果を全て8バイト単位で排他的論理和して生成したコンテンツ中間値を記録再生器300の内部メモリ307に格納されたコンテンツチェック値生成鍵Kicvcで暗号化して生成する。また、ブロックが暗号化されていない場合は、データ(平文)全体を8バイト単位で図36に示す改竄チェック値生成関数(DES-CBC-MAC、コンテンツチェック値生成鍵Kicvcを鍵とする)に入力して得た値として生成される。【0302】次にステップS115で記録再生器暗号処理部302の制御部306は、当該コンテンツチェック値と、ステップS102で記録再生器300の制御部301から受信したコンテンツブロック内のICVを比較し、その結果を記録再生器300の制御部301に渡す。これを受信した記録再生器300の制御部301は、検証に成功していた場合、次の検証対象コンテンツブロックを取り出して記録再生器300の記録再生器暗号処理部302に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理を繰り返す(ステップS116)。【0303】なお、ステップS104、S109、ステップS112、ステップS115のいずれかにおいて、チェック値の一致が得られなかった場合はエラーとしてダウンロード処理は終了する。【0304】次に、記録再生器300の記録再生器暗号処理部302は、ステップS106で復号化したブロック情報鍵Kbitとコンテンツ鍵Kconを、記録再生器暗号処理部302の暗号／復号化部308に、相互認証の際に共有しておいたセッション鍵Ksesで暗号化させる。記録再生器300

の制御部301は、セッション鍵Ksesで暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを記録再生器300の記録再生器暗号処理部302から読み出し、これらのデータを記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。【0305】次に、ステップS118において、記録再生器300から送信されてきたブロック情報鍵Kbitとコンテンツ鍵Kconを受信した記録デバイス400は、受信したデータを記録デバイス暗号処理部401の暗号／復号化部406に、相互認証の際に共有しておいたセッション鍵Ksesで復号化させ、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵Kstrで再び暗号化させ、記録再生器300の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400から保存鍵Kstrで再暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを読み出す。すなわち、配信鍵Kdisで暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconの鍵のかけかえを行なう。【0306】記録再生器300の制御部301は、データのヘッダ部の取扱方針(Usage Policy)から利用制限情報を取り出し、ダウンロードしたコンテンツが当該記録再生器300のみで利用できるか否かの判定を行なう。この判定は、ローカリゼーションフラグ(利用制限情報)=1に設定されている場合は、ダウンロードしたコンテンツが当該記録再生器300のみで利用でき、ローカリゼーションフラグ(利用制限情報)=0に設定されている場合は、ダウンロードしたコンテンツが別の同様な記録再生器300でも利用できることを示す。判定の結果、ローカリゼーションフラグ(利用制限情報)=1であった場合には、ステップS120に進む。【0307】ステップS120において、記録再生器300の制御部301は、記録再生器固有のチェック値を記録再生器300の記録再生器暗号処理部302に計算させる。記録再生器固有のチェック値は、図25に示すように記録再生器暗号処理部302の内部メモリ307に保存されている記録再生器に固有の記録再生器署名鍵Kdevを鍵とし、ステップS110で生成した中間チェック値をDESで暗号化して生成する。計算された記録再生器固有のチェック値ICVdevは、総チェック値ICVtの代わりに上書きされる。【0308】先に説明したJysは、配信システムに共通の署名またはICVをつけるために使用するシステム署名鍵であり、また、記録再生器署名鍵Kdevは、記録再生器毎に異なり、記録再生器が署名またはICVをつけるために使用する記録再生器署名鍵である。すなわち、システム署名鍵Ksysによって署名されたデータは、同じシステム署名鍵を有す

エック値A、チェック値Bと読み出したコンテンツデータに基づいて中間チェック値の生成を実行する。なお、コンテンツデータは暗号化されている場合でも、復号処理を行なわない。【0316】フォーマットタイプ2では、前述のマットタイプ0、1での処理のようにブロックデータの復号、コンテンツチェック値の照会処理を行なわないのと、迅速な処理が可能となる。【0317】ステップS111以降マットタイプ0、1における処理と同様であるので説明を省略する。【0318】以上が、フォーマットタイプ2におけるコンテンツデータのダウンロード処理の態様である。上述したようにフォーマットタイプ2のダウンロード処理は、フォーマットタイプ0、1での処理のようにブロックデータの復号、コンテンツチェック値の照会処理を行なないので、迅速な処理が可能となり、音楽データ等リアルタイム処理が要求されるデータ処理に適したフォーマットである。【0319】次に、フォーマットタイプ3におけるコンテンツデータのダウンロード処理について図4-1を用いて説明する。上記したフォーマットタイプ0、1、2のダウンロード処理と異なる点を中心に説明する。【0320】スマートフォーマットタイプ0、1、2のダウンロード処理と同様であるので説明は省略する。【0321】フォーマットタイプ3マットタイプ2における処理と共通する部分が多いが、1. フォーマットタイプ3はコンテンツ鍵を有しておらず、またブロック鍵K_{b1c}が記録デバイスにおいては保存鍵K_{s1t1r1}で暗号化されて格納される点がフォーマット1. タイプ2と異なる。【0322】フォーマットタイプ3のダウンロードにおけるフォーマットタイプ2と相違する点を中心として説明する。フォーマットタイプ3では、ステップS105の次ステップであるステップS161において、ブロック情報鍵の復号を行なう。記録再生器暗号処理部302の制御部306が、記録再生器暗号処理部302の2暗号/復号化部308を使って、ステップS105で生成した配信鍵K_{d1s1}を用いて、読み取り部304を介して受信したメディア500、または、通信部305を介して通信手段600から受信したデータのヘッダ部に格納されたブロック情報鍵K_{b1t1}の復号化処理を行う。フォーマットタイプ3では、データ中にコンテンツ鍵K_{c0n}が存在しないため、コンテンツ鍵K_{c0n}の復号化処理は実行されない。【0323】次のステップS107で復号したブロック情報鍵K_{b1t1}を用いてブロック情報の復号が実行され、さらに、ステップS162において、記録再生器暗号処理部302の制御部306

は、ブロック情報鍵K_{b i t}、およびブロック情報(BIT)から、チェック値B(IVB')を生成する。チェック値Bは、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵K_{i c v b}を鍵とし、ブロック情報鍵K_{b i t}、およびブロック情報(BIT)からなる排他的論理和値をDESで暗号化して生成する。次に、ステップS109において、チェック値Bとヘッダ(Header)内のIVBを比較し、一致していた場合にはステップS151へ進む。【0325】IVB、IVBは、ブロック情報鍵K_{b i t}、ブロック情報の改竄を検証するためのチェック値として機能する。生成したチェック値Bが、ヘッダ(Header)内に格納されたチェック値:IVBと一致した場合には、ブロック情報鍵K_{b i t}、ブロック情報の改竄はないと判断される。【0326】ステップS151～S112は、フォーマットタイプ2の処理と同様であるので説明を省略する。【0327】で読み出したコンテンツデータに含まれるブロック鍵K_{b l c}をステップS105で生成した配信鍵K_{d i s}によって復号する。【0328】次にステップS164では、00の記録再生器暗号処理部302が、ステップS161で復号化したブロック情報鍵K_{b i t}と、ステップS163で復号したブロック鍵K_{b l c}を、記録再生器暗号処理部302の暗号/復号化部308に、相互認証の際に共有しておいたセッション鍵K_{s e s}で暗号化させる。記録再生器300の制御部301は、セッション鍵K_{s e s}で暗号化されたブロック情報鍵K_{b i t}とブロック鍵K_{b l c}を記録再生器300の記録再生器暗号処理部302から読み出し、これらのデータを記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。【0329】次に、ステップS165～S170は、受信したデータを記録デバイス暗号処理部401の暗号/復号化部406に、相互認証の際に共有しておいたセッション鍵K_{s e s}で復号化させ、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵K_{s t r}で再暗号化させ、記録再生器300の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400から保存鍵K_{s t r}で再暗号化されたブロック情報鍵K_{b i t}とブロック鍵K_{b l c}を読み出す。すなわち、当初、配信鍵K_{d i s}で暗号化されたブロック情報鍵K_{b i t}とブロック鍵K_{b l c}を保存鍵K_{s t r}で再暗号化されたブロック情報鍵K_{b i t}とブロック鍵K_{b l c}へ置き換えを行なう。

【0329】以下のステップS119～S122は、前述のフォーマットタイプ0、1、2と同様であるので説明を省略する。【0330】以上が、フォーマットタイプ3におけるコンテンツデータのダウンロード処理の態様である。上述したようにフォーマットタイプ3のダウンロード処理は、フォーマットタイプ2と同様、ブロックデータの復号、コンテンツチェック値の照会処理を行なわないことで、迅速な処理が可能となり、音楽データ等リアルタイム処理が要求されるデータ処理に適したフォーマットである。また、ブロック鍵K_{b l c}により暗号化コンテンツを保護する範囲が局所化されているので、フォーマットタイプ2に比較して、よりセキュリティが高度となる。【0331】次に、フォーマットタイプ0～3各々における記録再生器300における記録デバイス400から記録再生器400の再生処理について図42～45のフローを用いて説明する。【0332】まず、フォーマットタイプ0におけるコンテンツの再生処理について図42を用いて説明する。【0333】バイス間における認証処理ステップであり、先に説明した図20の認証処理フローに従って実行される。【0334】スマートフラグがセットされると、記録再生器300は、ステップS202において、記録デバイス400から所定のフォーマットに従ったデータのヘッダを読み出し、記録再生器300の記録再生器暗号処理部302に送信する。【0335】次に、ステップS203において、暗号処理部302の制御部306が記録再生器暗号処理部302の暗号/復号化部308にチェック値Aを計算させる。チェック値Aは、先に説明した図23に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵K_{i c v a}を鍵とし、識別情報(Content ID)と取扱方針(Usage Policy)をメッセージとして計算される。次に、ステップS204において、計算されたチェック値Aとヘッダ(Header)内に格納されたチェック値:IVAを比較し、一致していた場合にはステップS205へ進む。【0336】取扱方針の改竄を検証するためのチェック値である。計算されたチェック値Aが、ヘッダ(Header)内に格納されたチェック値:IVAと一致した場合には、記録デバイス400に格納された識別情報、取扱方針の改竄はない判断される。【0337】次に、ステップS205において、記録再生器300の制御部301は、読み出したヘッダから記録デバイス固有の保存鍵K_{s t r}で暗号化されたブロック情報鍵K_{b i t}とコンテンツ鍵K_{c o n}を取り出し、

記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。【0338】記録再生器300は、受信したデータを記録デバイス暗号処理部401の暗号/復号化部406に、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵Kstrで復号化させ、相互認証の際に共有しておいたセッション鍵Ksesで再び暗号化させる。この処理は、前述した(9)相互認証後の鍵交換処理の欄で詳しく述べた通りである。【0340】記録再生器300の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400からセッション鍵Ksesで再暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを受信する。【0341】次に、記録再生器300の制御部301は、受信したセッション鍵Ksesで再暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを記録再生器300の記録再生器暗号処理部302に送信し、セッション鍵Ksesで再暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを受信した記録再生器300の記録再生器暗号処理部302は、記録再生器暗号処理部302の暗号/復号化部308に、セッション鍵Ksesで暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを、相互認証の際に共有しておいたセッション鍵Ksesで復号化させる。【0342】さらに、ステップS208において、記録再生器300の記録再生器暗号処理部302で、ステップS202で読み出しておいたブロック情報を復号化する。なお、記録再生器300の記録再生器暗号処理部302は、復号化したブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報BITを、ステップS202で読み出したヘッダに含まれるブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報BITに置き換えて保持しておく。また、記録再生器300の制御部301は、復号化されたブロック情報BITを記録再生器300の記録再生器暗号処理部302から読み出しておく。【0343】さらに、ステップS209において、記録再生器暗号処理部302の制御部306は、ブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報(BIT)から、チェック値B(IVb')を生成する。チェック値Bは、図24に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵Kicvbを鍵とし、ブロック情報鍵Kbit、コンテンツ鍵Kconおよびブロック情報(BIT)からなる排他的論理和値をDESで暗号化して生成する。次に、ステップS210において、チェック

値Bとヘッダ(Header)内のIVbを比較し、一致していた場合にはステップS211へ進む。【0344】チェック鍵Kbit、コンテンツ鍵Kcon、ブロック情報の改竄を検証するためのチェック値であり、生成したチェック値Bが、ヘッダ(Header)内に格納されたチェック値:IVbと一致した場合には、記録デバイス400に保存されたデータ中のブロック情報鍵Kbit、コンテンツ鍵Kcon、ブロック情報の改竄がないと判断される。【0345】ステップS211において、記録再生器300の制御部306は、記録再生器暗号処理部302の暗号/復号化部308に中間チェック値の計算をさせる。中間チェック値は、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されている総チェック値生成鍵Kicvtを鍵とし、検証したHeader内のチェック値A、チェック値B、ブロック情報中の全てのコンテンツチェック値をメッセージとして図7他で説明したIV計算方法に従って計算する。なお、生成した中間チェック値は、必要に応じて記録再生器300の記録再生器暗号処理部302に保持しておく。【0346】次に、ステップS212において、記録再生器300の制御部301は、記録デバイス400の外部メモリ402から読み出したデータのヘッダ部に含まれる取扱方針(Usage Policy)から利用制限情報を取り出し、再生予定のコンテンツが当該記録再生器300の復みで利用できる(利用制限情報が1)か、別の同様な記録再生器300でも利用できる(利用制限情報が0)か判定する。判定の結果、利用制限情報が1、すなわち再生コンテンツが当該記録再生器300のみで利用できる利用制限が設定されている場合には、ステップS213に進み、利用制限情報が0、すなわち別の同様な記録再生器300でも利用できる設定であった場合には、ステップS215に進む。なお、ステップS212の処理は暗号処理部302が行なってもよい。【0347】ステップS213の制御部301は、記録再生器固有のチェック値IVdev'を記録再生器300の記録再生器暗号処理部302に計算させる。記録再生器固有のチェック値IVdev'は、図25に示すように記録再生器暗号処理部302の内部メモリ307に保存されている記録再生器署名鍵Kdevを鍵とし、ステップS211で保持しておいた中間チェック値をDESで暗号化して生成する。【0348】一方ステップS215では、記録再生器300の制御部301は、記録再生器固有のチェック値IVdev'を記録再生器300の記録再生器暗号処理部302に計算した記録再生器固有のチェック値IVdev'をステップS202で読み出したヘッダ内のIVdevを比較し、一致していた場合には、ステップS217へ進む。

号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308に総チェック値ICVtの計算をさせる。総チェック値ICVt'は、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているシステム署名鍵Ksysを鍵とし、中間チェック値をDESで暗号化して生成する。次に、ステップS216において、生成した総チェック値ICVt'とヘッダ(Header)内のICVtを比較し、一致していた場合には、ステップS217へ進む。固有のチェック値ICVdevは、ICVa、ICVb、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成されたチェック値がヘッダ(Header)内に格納されたチェック値：ICVtまたはICVdevと一致した場合には、記録デバイス400に格納されたICVa、ICVb、各コンテンツブロックのチェック値全ての改竄はないと判断される。【0350】次に、ステップS218において暗号化されているか否かを判定し、暗号化されている場合は、記録再生器300の暗号処理部302においてブロックデータの復号を行なう。暗号化されていない場合は、ステップS219をスキップしてステップS220に進む。【0351】次に、ステップS220に進む。記録再生器300の制御部301は、ブロック情報(BIT)内のコンテンツブロック情報に基づいて、コンテンツブロックが検証対象になっているかいないか調べる。コンテンツブロックが検証対象になっている場合には、ヘッダ中のブロック情報中にコンテンツチェック値が格納されている。コンテンツブロックが検証対象になっていた場合には、ステップS221において、該当するコンテンツブロックのコンテンツチェック値ICVi'を計算させる。コンテンツブロックが検証対象になっていない場合には、ステップS221とS222をスキップしてステップS223に進む。【0352】コンテンツチェック値ICVi'を計算する。コンテンツチェック値ICVi'は、図36で説明したようにブロックが暗号化されている場合、コンテンツ鍵Kconで、入力されたコンテンツブロックをDESのCBCモードで復号化し、その結果を全て8バイト単位で排他的論理和して生成したコンテンツ中間値を記録再生器300の内部メモリ307に格納されたコンテンツチェック値生成鍵Kicvcで暗号化して生成する。また、ブロックが暗号化されていない場合は、データ(平文)全体を8バイト単位で図36に示す改竄チェック値生成関数(DES-CBC-MAC、コンテンツチェック値生成鍵Kicvcを鍵とする)に入力して得た値として生成される。

【0353】ステップS222においては、記録再生器暗号処理部302の制御部306は、生成したコンテンツチェック値 ICV_i' と、ステップS202で記録デバイス400から受信したヘッダ部に格納されたコンテンツチェック値 ICV_i とを比較し、その結果を記録再生器300の制御部301に渡す。これを受信した記録再生器300の制御部301は、検証に成功していた場合、ステップS223において、記録再生器システムR【0354】AM上に実行(再生)用コンテンツ平文データを格納する。記録再生器300の制御部301は、さらに次の検証対象コンテンツブロックを取り出して記録再生器300の記録再生器暗号処理部302に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理、RA M格納処理を繰り返す(ステップS224)。【0355】なお、0、ステップS214、ステップS216、ステップS222のいずれかにおいて、チェック値の一致が得られなかった場合はエラーとして再生処理は終了する。【0356】上記と判定されると、ステップS225に進み、コンテンツ(プログラム、データ)の実行、再生が開始される。【0357】以上が、フォーマットタイプ0におけるコンテンツデータの再生処理の様子である。【0358】次に、フォーマットデータの再生処理について図43を用いて説明する。上記したフォーマットタイプ0の再生処理と異なる点を中心に説明する。【0359】ステップS201～ステップS232の処理は、上記したフォーマットタイプ0の再生処理と同様であるので説明は省略する。【0360】フォーマットタイプ1において、暗号化パートの復号が実行され、パート ICV が生成される。さらに、ステップS232において、ブロック ICV_i' が生成される。先に説明したように、フォーマット・タイプ1においては、ブロック内のパートのうち少なくとも1つがチェック値 ICV_i の対象データである場合は、そのブロックに関してコンテンツチェック値 ICV_i が定義される。ブロック i におけるパート j のチェック値 $P-ICV_{i,j}$ は、パート j のチェック値が暗号化されている場合、平文(復号文)全体を8バイト単位で排他論理和した値をコンテンツチェック値生成鍵 K_{icvc} で暗号化した値として生成される。また、パート j が暗号化されていない場合は、データ(平文)全体を8バイト単位で図36に示す改竄チェック値生成関数(DES-CBC-MAC、コンテンツチェック値生成鍵 K_{icvc} を鍵とする)に入力して得た値として生成される。【0361】さらに、1つのブロック i 内にチェック象であることを示す[ICV フラグ=su b j e c t

o f I C V] であるパートが 1 つのみ存在する場合は、上述の手法で生成したチェック値 P-I C V i j をそのままブロックのチェック値 I C V i とし、また、1 つのブロック i 内にチェック対象であることを示す [I C V フラグ=s u b j e c t o f I C V] であるパートが複数存在する場合は、複数のパートチェック値 P-I C V i , j をパート番号順に連結したデータを対象にしてデータ（平文）全体を 8 バイト単位で図 3 6 に示す改竄チェック値生成関数（D E S-C B C-M A C、コンテンツチェック値生成鍵 K i c v c を鍵とする）に入力して得た値として生成される。これは、先に図 3 7 で説明した通りである。【0 3 6 1】フォーマットタイプ 1 が記録デバイスにおいては保存鍵 K s t r で暗号化されて格納される点がフォーマットタイプ 2 と異なる。【0 3 7 0】ステップ S 2 2 2 で実行されることになる。以下のステップ S 2 2 3 以下の処理はフォーマットタイプ 0 と同様であるので説明は省略する。【0 3 6 2】次に、フォーマットタイプ 3 、ステップ S 2 5 4 の処理は、前述のフォーマットタイプ 2 における対応処理と異なりコンテンツ鍵を含まない処理として構成されている。【0 3 7 1】ステップ S 2 0 0 の制御部 3 0 1 は、読み出したヘッダから記録デバイス固有の保存鍵 K s t r で暗号化されたブロック情報鍵 K b i t を取り出し、記録再生器 3 0 0 の記録デバイスコントローラ 3 0 3 を介して記録デバイス 4 0 0 に送信する。【0 3 7 2】記録再生器 3 0 0 から送信されたブロック情報鍵 K b i t を受信した記録デバイス 4 0 0 は、受信したデータを記録デバイス暗号処理部 4 0 1 の暗号/復号化部 4 0 6 に、記録デバイス暗号処理部 4 0 1 の内部メモリ 4 0 5 に保存してある記録デバイス固有の保存鍵 K s t r で復号化処理させ、相互認証の際に共有しておいたセッション鍵 K s e s で再暗号化させる。この処理は、前述した（9）相互認証後の鍵交換処理の欄で詳しく述べた通りである。【0 3 7 3】ステップ S 2 5 2 では、記録再生器 3 0 0 の記録デバイスコントローラ 3 0 3 を介し、記録デバイス 4 0 0 からセッション鍵 K s e s で再暗号化されたブロック情報鍵 K b i t を受信する。【0 3 7 4】次に、ステップ S 2 5 3 において、記録再生器 3 0 0 の制御部 3 0 1 は、受信したセッション鍵 K s e s で再暗号化されたブロック情報鍵 K b i t を記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 に送信し、記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 は、記録再生器暗号処理部 3 0 2 の暗号/復号化部 3 0 8 に、セッション鍵 K s e s で暗号化されたブロック情報鍵 K b i t を、相互認証の際に共有して

み出しと判定されると再生処理は終了する。【0 3 6 7】このようは、総チェック値等のチェック値検証処理を省略しており、高速な復号処理の実行に適している構成であり、音楽データ等リアルタイム処理が要求されるデータ処理に適したフォーマットである。【0 3 6 8】次にフォーマットタイプ 3 のデータの再生処理について図 4 5 を用いて説明する。上記したフォーマットタイプ 0, 1, 2 の再生処理と異なる点を中心に説明する。【0 3 6 9】フォーマットタイプ 3 、ステップ S 2 5 4 の処理は、前述のフォーマットタイプ 2 における処理と共通する部分が多いが、フォーマットタイプ 3 は図 3 5 において説明したようにコンテンツ鍵を有しておらず、またブロック鍵 K b l c が記録デバイスにおいては保存鍵 K s t r で暗号化されて格納される点がフォーマットタイプ 2 と異なる。【0 3 7 0】ステップ S 2 2 2 で実行されることになる。以下のステップ S 2 2 3 以下の処理はフォーマットタイプ 0 と同様であるので説明は省略する。【0 3 6 2】次に、フォーマットタイプ 3 、ステップ S 2 5 4 の処理は、前述のフォーマットタイプ 2 における対応処理と異なりコンテンツ鍵を含まない処理として構成されている。【0 3 7 1】ステップ S 2 0 0 の制御部 3 0 1 は、読み出したヘッダから記録デバイス固有の保存鍵 K s t r で暗号化されたブロック情報鍵 K b i t を取り出し、記録再生器 3 0 0 の記録デバイスコントローラ 3 0 3 を介して記録デバイス 4 0 0 に送信する。【0 3 7 2】記録再生器 3 0 0 から送信されたブロック情報鍵 K b i t を受信した記録デバイス 4 0 0 は、受信したデータを記録デバイス暗号処理部 4 0 1 の暗号/復号化部 4 0 6 に、記録デバイス暗号処理部 4 0 1 の内部メモリ 4 0 5 に保存してある記録デバイス固有の保存鍵 K s t r で復号化処理させ、相互認証の際に共有しておいたセッション鍵 K s e s で再暗号化させる。この処理は、前述した（9）相互認証後の鍵交換処理の欄で詳しく述べた通りである。【0 3 7 3】ステップ S 2 5 2 では、記録再生器 3 0 0 の記録デバイスコントローラ 3 0 3 を介し、記録デバイス 4 0 0 からセッション鍵 K s e s で再暗号化されたブロック情報鍵 K b i t を受信する。【0 3 7 4】次に、ステップ S 2 5 3 において、記録再生器 3 0 0 の制御部 3 0 1 は、受信したセッション鍵 K s e s で再暗号化されたブロック情報鍵 K b i t を記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 に送信し、記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 は、記録再生器暗号処理部 3 0 2 の暗号/復号化部 3 0 8 に、セッション鍵 K s e s で暗号化されたブロック情報鍵 K b i t を、相互認証の際に共有して

おいたセッション鍵K_{s e s}で復号化させる。【0375】さ化したブロック情報鍵K_{b i t}で、ステップS202で読み出しておいたブロック情報を復号化する。なお、記録再生器300の記録再生器暗号処理部302は、復号化したブロック情報鍵K_{b i t}およびブロック情報B_{I T}を、ステップS202で読み出したヘッダに含まれるブロック情報鍵K_{b i t}およびブロック情報B_{I T}に置き換えて保持しておく。また、記録再生器300の制御部301は、復号化されたブロック情報B_{I T}を記録再生器300の記録再生器暗号処理部302から読み出しておく。【0376】さらに、ステップS254において、記録再生器暗号処理部302の制御部306は、ブロック情報鍵K_{b i t}およびブロック情報(B_{I T})から、チェック値B(I_{C V b'})を生成する。チェック値Bは、図24に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵K_{i c v b}を鍵とし、ブロック情報鍵K_{b i t}およびブロック情報(B_{I T})からなる排他的論理和値をDESで暗号化して生成する。次に、ステップS210において、チェック値Bとヘッダ(Header)内のI_{C V b}を比較し、一致していた場合にはステップS211へ進む。ブロック鍵が記録デバイスでの格納時に保存鍵によって暗号化されるため、記録デバイス400における保存鍵での復号処理、およびセッション鍵での暗号化処理、さらに、記録再生器300でのセッション鍵での復号処理が必要となる。これらの一連の処理がステップS255、ステップS256で示した処理ステップである。【0377】の制御部301は、ステップS217で読み出したブロックから記録デバイス固有の保存鍵K_{s t r}で暗号化されたブロック鍵K_{b l c}を取り出し、記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。【0378】記録再生器300から送信したブロック鍵K_{b l c}を受信した記録デバイス400は、受信したデータを記録デバイス暗号処理部401の暗号/復号化部406に、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵K_{s t r}で復号化処理させ、相互認証の際に共有しておいたセッション鍵K_{s e s}で再暗号化させる。この処理は、前述した「(9) 相互認証後の鍵交換処理」の欄で詳しく述べた通りである。【0379】ステップS256の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400からセッション鍵K_{s e s}で再暗号化されたブロック鍵K_{b l c}を受信する。

【0381】次に、ステップS257において、記録再生器300の暗号処理部306によるブロック鍵K_{b l c}のセッション鍵K_{s e s}を用いた復号処理が実行される。【0382】次に、ステップS242において、ステップS257で復号されたブロック鍵K_{b l c}を用いてブロックデータの復号処理が実行される。さらに、ステップS243において、コンテンツ(プログラム、データ)の実行、再生処理が実行される。ステップS217～ステップS243の処理が全ブロックについて繰り返し実行される。ステップS244において全ブロック読み出しと判定されると再生処理は終了する。【0383】以上の大枠の処理が実行されると、各コンテンツの再生処理である。総チェック値の検証処理が省略された点でフォーマットタイプ2と類似するが、ブロック鍵の鍵交換処理を含む点でフォーマットタイプ2に比較して、さらにセキュリティ・レベルの高い処理構成となっている。【0384】(1) コンテンツプロバイエック値(I_{C V})生成処理態様上述の実施例中において、各種の検証処理が、コンテンツのダウンロード、または再生処理等の段階で実行されることを説明してきた。ここでは、これら各チェック値(I_{C V})生成処理、検証処理の態様について説明する。【0385】まず、実施例で説明していくと、本発明のデータ処理装置において利用されるチェック値I_{C V}には以下のものがある。【0386】チェック値A, I_{C V a}：コンテンツデータ中の識別情報、取扱方針の改竄を検証するためのチェック値。チェック値B, I_{C V b}：ブロック情報鍵K_{b i t}、コンテンツ鍵K_{c o n}、ブロック情報の改竄を検証するためのチェック値。コンテンツチェック値I_{C V i}：コンテンツの各ブロックの改竄を検証するためのチェック値。総チェック値I_{C V b}、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。再生器固有チェック値I_{C V t}送信フラグが1にセットされている場合、すなわち、コンテンツが記録再生器固有に利用可能であることを示している場合に、総チェック値I_{C V t}に置き換えるチェック値であり、前述のチェック値A: I_{C V a}、チェック値B: I_{C V b}、さらにコンテンツのチェック対象となっている各ブロックに含まれるチェック値I_{C V i}全体に対するチェック値として生成される。フォーマットによっては、I_{C V t}、I_{C V d e v}がチェックする対象に含まれるのは、各コンテンツブロックのチェック

値ではなく、コンテンツそのものとなる場合もある。【038】録再生器利用者）、すなわち検証者の有するICV生成者の公開鍵は秘密にする必要がなく、管理は容易となる。ICVの生成、管理が1つのエンティティにおいて実行される場合等、ICVの生成、管理が高いセキュリティ管理レベルで行われている場合に適した態様である。【0392】図48は、コンテンツ提供者または管理者であるICVの生成者が公開鍵暗号系のデジタル署名によりICVを生成して、生成したICVをコンテンツと共にコンテンツ利用者、すなわち検証者に提供し、さらに、検証者が検証に用いる公開鍵を公開鍵証明書（例えば図14参照）に格納してコンテンツデータと共に記録再生器利用者、すなわち検証者に提供する。ICVの生成者が複数存在する場合には、各生成者は、公開鍵の正当性を証明するデータ（公開鍵証明書）を鍵管理センタに作成してもらう。【0393】ICVの検証者であるコンテンツは、鍵管理センタの公開鍵を持ち、検証者は公開鍵証明書の検証を鍵管理センタの公開鍵によって実行し、正当性が確認されたら、その公開鍵証明書に格納されたICVの生成者の公開鍵を取り出す。さらに、取り出したICVの生成者の公開鍵を用いてICVの検証を実行する。【0394】この方法は、ICVの生成者が複数あり、それらの管理を実行するセンタによる管理の実行システムが確立している場合に有効な態様である。【0395】（12）構成次に、本発明のデータ処理システムにおける特徴的な構成の1つである、マスク鍵に基づく各種暗号処理用鍵の生成構成について説明する。【0396】先に図18を用いて説明のデータ処理装置における記録再生器300の内部メモリには、様々なマスク鍵が格納され、これらの各マスク鍵を用いて、例えば認証鍵K_{ack}を生成（数3参照）したり、あるいは配達鍵K_{dis}を生成（数4参照）する構成となっている。【0397】従来、1対1のエンティティコンテンツプロバイダとコンテンツ利用者間、あるいは、上述の本発明のデータ処理装置における記録再生器300と記録メディア400との間において暗号通信、相互認証、MAC生成、検証等を行なう際には、各エンティティに共通な秘密情報、例えば鍵情報を保持させていた。また、1対多の関係、例えば1つのコンテンツプロバイダに対する多数のコンテンツ利用者、あるいは1つの記録再生器に対する多数の記録メディア等の関係においては、すべてのエンティティ、すなわち多数のコンテンツ利用者、あるいは多数の記録メディアにおいて共有させた秘密情報、例えば鍵情報を格納保持させる構成とするか、あるいは、1つのコンテンツプロバイダが多

数のコンテンツ利用者各々の秘密情報(e x. 鍵)を個別に管理し、これを各コンテンツ利用者に応じて使い分けていた。【0398】しかしながら、上記のような1対多の関係がある場合、すべてが共有する秘密情報(e x. 鍵)を所有する構成においては、1箇所の秘密漏洩が発生すると同じ秘密情報(e x. 鍵)を利用している者すべてに影響が及ぶという欠点がある。また、1つの管理者、例えばコンテンツプロバイダが多数のコンテンツ利用者各々の秘密情報(e x. 鍵)を個別に管理し、これを各コンテンツ利用者に応じて使い分ける構成とすると、すべての利用者を識別し、かつその識別データに固有の秘密情報(e x. 鍵)を対応づけたりストが必要となり、利用者の増大に伴うリストの保守管理の負担が増加するという欠点がある。【0399】本発明のデータ処理装置においては、このようなエンティティ間における秘密情報の共有における従来の問題点をマスター鍵の保有、およびマスター鍵から各種の個別鍵を生成する構成により解決した。以下、この構成について説明する。【0400】本発明のデータ処理装置やコンテンツを格納したメディア、または記録再生器間での各種の暗号処理、認証処理等において異なる個別の鍵が必要になる場合、その個別の鍵を、デバイスやメディアが固有に持つ識別子データ(ID)などの個別情報と記録再生器300内であらかじめ決められた個別鍵生成方式を用いて生成する。この構成により万が一、生成された個別の鍵が特定された場合でもマスター鍵の漏洩を防止すれば、システム全体への被害を防ぐことが可能となる。またマスター鍵によって鍵を生成する構成により対応づけリストの管理も不要となる。【0401】する。まず、図49に各種の鍵を記録再生器300の有する各種のマスター鍵を用いて生成する構成を説明する図を示す。図49のメディア500、通信手段600からは、すでに説明した実施例と同様、コンテンツが入力される。コンテンツはコンテンツ鍵Kconによって暗号化され、またコンテンツ鍵Kconは、配送鍵Kdisによって暗号化されている。【0402】例えば、記録再生器300、通信手段600からコンテンツを取り出して、記録デバイス400にダウンロードしようとする場合、先の図22、図39～41において説明したように、記録再生器300は、コンテンツ鍵を暗号化している配送鍵Kdisを取得することが必要となる。このKdisをメディア500、通信手段600から直接取得したり、あるいは予め記録再生器300が取得して記録再生器300内のメモリに格納しておくことも可能であるが、このような鍵の多数のユーザに対する配布構成は、先にも説明したようにシステム全体に影響を及ぼす漏洩の可能性

がある。【0403】本発明のデータ処理システムでは、この配送鍵Kdisを図49の下部に示すように、記録再生器300のメモリに格納された配送鍵用マスター鍵MKdisと、コンテンツIDに基づく処理、すなわちKdis=DES(MKdis, コンテンツID)を適用して配送鍵Kdisを生成する構成としている。本構成によれば、メディア500、通信手段600からコンテンツを供給するコンテンツプロバイダとそのコンテンツ利用者である記録再生器300間におけるコンテンツ配布構成において、コンテンツプロバイダが多数存在した場合であっても、個々の配送鍵Kdisをメディア、通信媒体等を介して流通させる必要もなく、また、各記録再生器300に格納する必要もなく、セキュリティを高度に保つことが可能となる。【0404】次に、認証鍵Kakeの生成する。先に説明した図22、図39～41の記録再生器300から記録メディア400に対するダウンロード処理、あるいは図28、図42～45で説明した記録メディア400に格納されたコンテンツを記録再生器300において実行、再生する場合、記録再生器300と記録メディア400間における相互認証処理(図20参照)が必要となる。【0405】図20で説明したように、この認証において記録再生器300は認証鍵Kakeが必要となる。記録再生器300は、認証鍵を例えば記録メディア400から直接取得したり、あるいは予め記録再生器300が取得して記録再生器300内のメモリに格納しておくことも可能であるが、上述の配送鍵の構成と同様、このような鍵の多数のユーザに対する配布構成は、システム全体に影響を及ぼす漏洩の可能性がある。【0406】本発明の認証鍵Kakeを図49の下部に示すように、記録再生器300のメモリに格納された認証鍵用マスター鍵MKakeと、記録デバイス識別ID:IDmemに基づく処理、すなわちKake=DES(MKake, IDmem)によって認証鍵Kakeを求める構成としている。【0407】記録再生器300から記録メディア400に対するダウンロード処理、あるいは図28、図42～45で説明した記録メディア400に格納されたコンテンツを記録再生器300において実行、再生する場合、記録再生器300に利用可能なコンテンツである場合の記録再生器固有チェック値ICVdevの生成処理に必要となる記録再生器署名鍵Kdevについても上述の配送鍵、認証鍵と同様の構成とすることができます。上述の実施例中では、記録再生器署名鍵Kdevは内部メモリに格納する構成としていたが、記録再生器署名鍵用マスター鍵MKdevをメモリに格納し、記録再生器署名鍵Kdevは内部メモリに格納せず、必要に応じて図49の下部に示すように記録

再生器識別子： ID_{dev} と記録再生器署名鍵用マスター鍵 MK_{dev} に基づいて、 $K_{dev} = DES(MK_{dev}, ID_{dev})$ によって記録再生器署名鍵 K_{dev} を求める構成とすることで、記録再生器署名鍵 K_{dev} を機器個別に持たせる必要がなくなるという利点が挙げられる。【0408】このように、本発明のデータ処理装置においては、プロバイダと記録再生器、あるいは記録再生器と記録デバイス間のような2つのエンティティ間における暗号情報処理に関する手続きに必要な鍵等の情報をマスター鍵と各 ID から逐次的に生成する構成としたので、鍵情報が各エンティティから漏洩した場合でも、個別の鍵による被害の範囲はより限定され、また前述したような個別のエンティティごとの鍵リストの管理も不要となる。【0409】本構成に関する複数の処理例について図50を示して説明する。図50は、コンテンツ製作または管理者におけるマスター鍵を用いたコンテンツ等の暗号化処理と、ユーザデバイス、例えば上述の実施例における記録再生器300におけるマスター鍵を用いた暗号化データの復号処理例である。【0410】コンテンツ製作または管理者におけるマスター鍵を用いたコンテンツ等の暗号化処理と、ユーザデバイス、例えば上述の実施例における記録再生器300におけるマスター鍵を用いた暗号化データの復号処理例である。【0411】一方、例えば記録再生器300等のユーザデバイス側では、ステップS504において、メディア、通信手段等を介して受領したコンテンツデータ中からコンテンツIDを読み出す。次に、ステップS505において、読み出したコンテンツIDと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、配送鍵 K_{dis} を得るものである場合は、例えば配送鍵 $K_{dis} = DES(MK_{dis}, ID_{dis})$ となる。ステップS506で、この鍵を用いてコンテンツを復号し、ステップS507で復号コンテンツの利用、すなわち再生またはプログラムを実行する。【0412】この例においては、図50下段に、コンテンツ製作または管理者と、ユーザデバイスの双方がマスター鍵（例えば配送鍵生成用マスター鍵 MK

dis ）を有し、コンテンツの暗号化、復号に必要な配送鍵を逐次的にそれぞれの所有するマスター鍵と各 ID (コンテンツ ID) に基づいて生成する。【0413】このシステムに漏洩した場合、そのコンテンツの復号が第三者において可能となるが、コンテンツ ID の異なる他のコンテンツの復号は防止することが可能であるため、1つのコンテンツ鍵の漏洩がシステム全体に及ぼす影響を最小限にできるという効果がある。また、ユーザデバイス側、すなわち記録再生器において、コンテンツ毎の鍵の対応付けリストを保持する必要がないという効果もある。【0414】次に図51を用いて、コンテンツ製作または管理者が複数のマスター鍵を所有して、コンテンツの配信対象に応じた処理を実行する例について説明する。【0415】図51は、コンテンツに対する識別子 (コンテンツ ID) を付与するステップである。ステップS512は、コンテンツ製作または管理者の有する複数のマスター鍵（例えば複数の配送鍵生成用マスター鍵 MK_{dis} ）から1つのマスター鍵を選択するステップである。この選択処理は図52を用いてさらに説明するが、コンテンツの利用者の国ごと、機種ごと、あるいは機種のバージョンごとなどに対応付けて予め適用するマスター鍵を設定しておき、その設定に従って実行するものである。【0416】次に、ステップS513では、ステップS512で選択したマスター鍵と、ステップS511で決定したコンテンツ ID に基づいて暗号化用の鍵を生成する。これは例えば、配送鍵 $K_{disi} = DES(MK_{disi}, ID_{disi})$ によって生成する。次に、ステップS514はコンテンツの一部、または全部を鍵（例えば配送鍵 K_{disi} ）によって暗号化するステップである。コンテンツ製作者は、ステップS515において、コンテンツ ID と、使用したマスター鍵識別情報と、暗号化コンテンツを1つの配布単位として暗号化処理を行なったコンテンツをDVD等のメディア、通信手段等を介して配信する。【0417】一方、例えば記録再生器300等のユーザデバイス側では、ステップS516において、DVD等のメディア、通信手段等を介して配信されたコンテンツデータ中のマスター鍵識別情報に対応するマスター鍵を自己が所有するか否かについて判定する。コンテンツデータ中のマスター鍵識別情報に対応するマスター鍵を持たない場合は、その配布コンテンツは、そのユーザデバイスにおいては利用できないものであり、処理は終了する。【0418】配信されたコンテンツデータ中のマスター鍵識別情報に対応するマスター鍵を自己が所有する場合

は、ステップS 517において、メディア、通信手段等を介して受領したコンテンツデータ中からコンテンツIDを読み出す。次に、ステップS 518において、読み出したコンテンツIDと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、配送鍵K_{d i s i}を得るものである場合は、例えば配送鍵K_{d i s i}=DES (MK_{d i s i}, コンテンツID)となる。ステップS 519で、この鍵を用いてコンテンツを復号し、ステップS 520で復号コンテンツの利用、すなわち再生またはプログラムを実行する。【0419】この例においては、図51下段に示すように、コンテンツ製作または管理者は、複数のマスター鍵、例えば複数の配送鍵生成用マスター鍵MK_{d i s 1}～nからなるマスター鍵セットを有する。一方、ユーザデバイスには1つのマスター鍵例えば1つの配送鍵生成用マスター鍵KK_{d i s i}を有し、コンテンツ製作または管理者がMK_{d i s i}を用いて暗号化処理している場合のみ、ユーザデバイスは、そのコンテンツを復号して利用することができる。【0420】この図51のフローして、国毎に異なるマスター鍵を適用した例を図52に示す。コンテンツプロバイダは、マスター鍵MK_{1～n}を有し、MK₁は日本向けのユーザデバイスに配信するコンテンツの暗号化処理を実行する鍵生成に用いる。例えば、コンテンツIDとMK₁から暗号化鍵K₁を生成してK₁によってコンテンツを暗号化する。また、MK₂はUS向けのユーザデバイスに配信するコンテンツの暗号化処理を実行する鍵生成に用い、MK₃はEU(ヨーロッパ)向けのユーザデバイスに配信するコンテンツの暗号化処理を実行する鍵生成に用いるよう設定している。【0421】一方、日本向けユーザデバイス、具体的には日本で販売されるPCまたはゲーム機器等の記録再生器には、マスター鍵MK₁がその内部メモリに格納され、US向けユーザデバイスには、マスター鍵MK₂がその内部メモリに格納され、EU向けユーザデバイスには、マスター鍵MK₃がその内部メモリに格納されている。【0422】このような構成において、コンテンツプロバイダは、コンテンツを利用可能なユーザデバイスに応じて、マスター鍵MK_{1～n}から、マスター鍵を選択的に使用してユーザデバイスに配信するコンテンツの暗号化処理を実行する。例えばコンテンツを日本向けのユーザデバイスのみ利用可能とするためには、マスター鍵MK₁を用いて生成された鍵K₁によってコンテンツを暗号化する。この暗号化コンテンツは、日本向けユーザデバイスに格納されたマスター鍵MK₁を用いて復号可能、すなわち復号鍵を生成可能であるが、他のUS、またはEU向けのユーザデバイスに格納されたマスター鍵

MK₂, MK₃からは鍵K₁を得ることができないので、暗号化コンテンツの復号は不可能となる。【0423】このよのマスター鍵を選択的に使用することにより、様々なコンテンツの利用制限を設定することができる。図52では、ユーザデバイスの国別にマスター鍵を区別する例を示したが、前述のように、ユーザデバイスの機種に応じて、あるいはバージョンに応じてマスター鍵を切り換える等、様々な利用形態が可能である。【0424】次に、図53になわちメディアIDとマスター鍵を組み合わせた処理例を示す。ここで、メディアとは例えばDVD、CD等のコンテンツを格納したメディアである。メディアIDは、1つ1つのメディアごとに固有としてもよいし、たとえば、映画などのコンテンツのタイトルごとに固有としてもよいし、メディアの製造ロットごとに固有としてもよい。このようにメディアIDの割り当て方法としては様々な方法を用いることができる。【0425】メディア製作プロセスS 521は、メディアに対する識別子(メディアID)を決定するステップである。ステップS 522は、メディア製作または管理者の有するマスター鍵とメディアIDに基づいてメディア内の格納コンテンツ等を暗号化する鍵を生成するステップである。これは例えば、配送鍵K_{d i s}を生成する工程とすれば、前述のK_{d i s}=DES (MK_{d i s}, メディアID)によって配送鍵K_{d i s}を生成する。次に、ステップS 523は、メディア格納コンテンツの一部、または全部を鍵(例えば配送鍵K_{d i s})によって暗号化するステップである。メディア製作者は、このようなステップを経て暗号化処理を行なったコンテンツ格納メディアを供給する。【0426】デバイス側では、ステップS 524において、供給されたメディアからメディアIDを読み出す。次に、ステップS 525において、読み出したメディアIDと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、配送鍵K_{d i s}を得るものである場合は、例えば配送鍵K_{d i s}=DES (MK_{d i s}, メディアID)となる。ステップS 526で、この鍵を用いてコンテンツを復号し、ステップS 527で復号コンテンツの利用、すなわち再生またはプログラムを実行する。【0427】この例においては、図53下段に、メディア製作または管理者と、ユーザデバイスの双方がマスター鍵(例えば配送鍵生成用マスター鍵MK_{d i s})を有し、コンテンツの暗号化、復号に必要な配送鍵を逐次的にそれぞれの所有するマスター鍵と各ID(メディアID)に基づいて生成する。【0428】このシステムに漏洩した場合、そのメディア内のコンテンツの復

号が第三者において可能となるが、メディアIDの異なる他のメディアに格納されたコンテンツの復号は防止することが可能であるため、1つのメディア鍵の漏洩がシステム全体に及ぼす影響を最小限にすることができるという効果がある。また、ユーザデバイス側、すなわち記録再生器において、メディア毎の鍵の対応付けリストを保持する必要がないという効果もある。また、1つのメディア鍵で暗号化されるコンテンツサイズは、そのメディア内に格納可能な容量に制限されるため、暗号文攻撃のために必要な情報量に達する可能性は少なく、暗号解読の可能性を低減させることができる。【0429】次に、すなわち記録再生器IDとマスター鍵を組み合わせた処理例を示す。【0430】記録再生器利用者におけるステップ1は、記録再生器の例えば内部メモリに格納されたマスター鍵と記録再生器IDとに基づいてコンテンツ等を暗号化する鍵を生成するステップである。これは例えば、コンテンツ鍵K_{con}を生成する工程とすれば、K_{con}=DES (MK_{con}, 記録再生器ID) によってコンテンツ鍵K_{con}を生成する。次に、ステップS532は、格納するコンテンツの一部、または全部を鍵（例えば配達鍵K_{con}）によって暗号化するステップである。ステップS533は、暗号化コンテンツを例えばハードディスク等の記録デバイスに格納する。【0431】者側では、コンテンツを格納した記録再生器利用者から格納データの復旧を依頼されると、ステップS534において、記録再生器から、記録再生器IDを読み出す。次に、ステップS535において、読み出した記録再生器IDと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、コンテンツ鍵K_{con}を得るものである場合は、例えばコンテンツ鍵K_{con}=DES (MK_{con}, 記録再生器ID) となる。ステップS536で、この鍵を用いてコンテンツを復号する。【0432】この例においては、図54において、記録再生器利用者と、システム管理者の双方がマスター鍵（例えばコンテンツ鍵生成用マスター鍵MK_{con}）を有し、コンテンツの暗号化、復号に必要な配達鍵を逐次的にそれぞれの所有するマスター鍵と各ID（記録再生器ID）に基づいて生成する。【0433】このシステムに漏洩した場合、そのコンテンツの復号が第三者において可能となるが、記録再生器IDの異なる他の記録再生器用に暗号化されたコンテンツの復号は防止することが可能であるため、1つのコンテンツ鍵の漏洩がシステム全体に及ぼす影響を最小限にすることができるという効果がある。また、システム管理側、ユーザデバイス側両者において、コンテンツ毎の鍵の対応付けリスト

を保持する必要がないという効果もある。【0434】図55は、リカード等の記録デバイスと、ホストデバイス、例えば記録再生器間における相互認証処理に用いる認証鍵をマスター鍵に基づいて生成する構成である。先に説明した認証処理（図20参照）では、スレーブデバイスの内部メモリに認証鍵を予め格納した構成としてあるが、これを図55に示すように認証処理時にマスター鍵に基づいて生成する構成とすることができる。【0435】例えば記録デノスは、認証処理開始前の初期化処理として、ステップS541において、記録デバイスであるスレーブデバイスの内部メモリに格納したマスター鍵とスレーブデバイスIDに基づいて相互認証処理に用いる認証鍵K_{ake}を生成する。これは例えば、K_{ake}=DES (MK_{ake}, スレーブデバイスID) によって生成する。次に、ステップS542において、生成した認証鍵をメモリに格納する。【0436】一方、例えば記録再生器等のホストラス側では、ステップS543において、装着された記録デバイス、すなわちスレーブデバイスから、通信手段を介してスレーブデバイスIDを読み出す。次に、ステップS544において、読み出したスレーブデバイスIDと所有する認証鍵生成用マスター鍵に基づいて相互認証処理に適用する認証鍵を生成する。この生成処理は、例えれば認証鍵K_{ake}=DES (MK_{ake}, スレーブデバイスID) となる。ステップS545で、この認証鍵を用いて認証処理を実行する。【0437】この例においては、図54において、スレーブデバイスと、マスターデバイスの双方がマスター鍵、すなわち認証鍵生成用マスター鍵MK_{ake}を有し、相互認証処理に必要な認証鍵を逐次的にそれぞれの所有するマスター鍵とスレーブデバイスIDに基づいて生成する。【0438】このシステムでは、万が一認証鍵が漏洩した場合、その認証鍵は、そのスレーブデバイスのみに有効であるため、他のスレーブデバイスとの関係において生成する。【0439】このように、本発明のデータ処理装置においては、コンテンツプロバイダと記録再生器、あるいは記録再生器と記録デバイス間のような2つのエンティティ間における暗号情報処理に関する手続きに必要な鍵等の情報をマスター鍵と各IDから逐次的に生成する構成とした。従って、鍵情報が各エンティティから漏洩した場合でも、個別の鍵による被害の範囲はより限定され、また前述したような個別のエンティティごとの鍵リストの管理も不要となる。【0440】(13) 暗号処理における暗号

上述した実施例において、記録再生器300と記録デバイス400間での暗号処理は、説明を理解しやすくするため、主として、先に図7を用いて説明したシングルDES構成による暗号処理を用いた例について説明してきた。しかしながら、本発明のデータ処理装置において適用される暗号化処理方式は上述したシングルDES方式に何ら限定されるものではなく、必要なセキュリティ状態に応じた暗号化方式を採用することが可能である。【0444】のようなトリプルDES方式を適用してもよい。例えば図3に示す記録再生器300の暗号処理部302と、記録デバイス400の暗号処理部401の双方において、トリプルDES方式を実行可能な構成とし、図8～図10で説明したトリプルDES方式による暗号処理に対応する処理を実行する構成が可能である。【0442】しかしながら、シングルDES方式による64ビット鍵構成とする場合もあり、また、セキュリティを優先してコンテンツ鍵KconをトリプルDES方式による128ビット、または192ビット鍵構成とする場合もある。従って、記録再生器300の暗号処理部302と、記録デバイス400の暗号処理部401の構成をトリプルDES方式、シングルDES方式いずれか一方の方式にのみ対応可能な構成とすることは好ましくない。従って、記録再生器300の暗号処理部302と、記録デバイス400の暗号処理部401は、シングルDES、トリプルDESいずれの方式にも対応可能とする構成が望ましい。【0443】暗号処理部302と、記録デバイス400の暗号処理部401の暗号処理構成をシングルDES方式、トリプルDES方式の双方を実行可能な構成とするためには、それぞれの別の回路、ロジックを構成しなければならない。例えば、記録デバイス400においてトリプルDESに対応する処理を実行するためには、先の図29に示すコマンドレジスタにトリプルDESの命令セットを新たに格納することが必要となる。これは記録デバイス400に構成する処理部の複雑化を招くこととなる。【0444】そこで、記録デバイス400側の暗号処理部401の有するロジックをシングルDES構成として、かつトリプルDES暗号化処理に対応した処理が実行可能で、トリプルDES方式による暗号化データ(鍵、コンテンツ等)を記録デバイスの外部メモリ402に格納することを可能とした構成を提案する。【0445】例えば図32に示すデータフォーマットタイプ0の例において、記録再生器300から記録デバイス400に対してコンテンツデータのダウンロードを実行する際、先に説明したデータフォーマットタイプ0のダウンロードのフローを示す図39のステップS101で認証

処理を実行し、ここでセッション鍵Ksesを生成する。さらに、ステップS117において、記録再生器300側の暗号処理部302においてセッション鍵Ksesによるコンテンツ鍵Kconの暗号化処理が実行され、この暗号化鍵が記録デバイス400に通信手段を介して転送され、ステップS118において、この暗号化鍵を受信した記録デバイス400の暗号処理部403がセッション鍵Ksesによるコンテンツ鍵Kconの復号処理を実行し、さらに、保存鍵Kstrによるコンテンツ鍵Kconの暗号化処理を実行して、これを記録再生器300の暗号処理部302に送信し、その後、記録再生器300がデータフォーマットを形成(ステップS121)してフォーマット化されたデータを記録デバイス400に送信し、記録デバイス400が受信したデータを外部メモリ402に格納する処理を行なっている。【0446】18間において実行される記録デバイス400の暗号処理部401での暗号処理をシングルDES、またはトリプルDESいずれかの方式を選択的に実行可能な構成とすれば、コンテンツ提供業者がトリプルDESにしたがったコンテンツ鍵Kconを用いたコンテンツデータを提供する場合も、またシングルDESにしたがったコンテンツ鍵Kconを用いたコンテンツデータを提供する場合も、いずれの場合にも対応可能となる。【0447】図56に記録再生器300の暗号処理部302と、記録デバイス400の暗号処理部401との双方を用いてトリプルDES方式に従った暗号処理方法を実行する構成を説明するフローを示す。図56では、一例として記録再生器300からコンテンツデータを記録デバイス400にダウンロードする際に実行される保存鍵Kstrを用いたコンテンツ鍵Kconの暗号化処理例であり、コンテンツ鍵KconがトリプルDES方式による鍵である場合の例を示している。なお、ここでは、コンテンツ鍵Kconを代表して、その処理例を示すが、他の鍵、またはコンテンツ等、その他のデータについても同様の処理が可能である。【0448】トリプルDES方式においては、先の図8～10において説明したように、シングルDESでは64ビット鍵、トリプルDES方式による場合は、128ビット、または192ビット鍵構成として、2つ、または3つの鍵が用いられる処理である。これら3つのコンテンツ鍵をそれぞれKcon1、Kcon2、(Kcon3)とする。Kcon3は用いられない場合もあるので、かっこで示している。【0449】図56の処理について説明S301は記録再生器300と、記録デバイス400間での相互認証処理ステップである。この相互認証処理ステップは、先に説明した図20の処理によって実行される。なお、この認証処理の際、セッション鍵Ksesが

生成される。【0450】ステップS301の認証処理が終了し、記録再生器300から読み出し、これらのデータを記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。【0451】次に、ステップS303において、各チェック値、チェック値A、チェック値B、コンテンツチェック値、総チェック値、各ICVの照合処理が実行される。【0452】これ終了し、データ改竄がないと判定されると、ステップS303に進み、記録再生器300において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308を使って、先に取り出したまたは生成した配達鍵Kdisを用いて、受信したメディア500、または、通信部305を介して通信手段600から受信したデータのヘッダ部に格納されたコンテンツ鍵Kconの復号化処理を行う。この場合のコンテンツ鍵は、トリプルDES方式による鍵であり、コンテンツ鍵Kcon1, Kcon2, (Kcon3)である。【0453】次に、ステップS304において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308において、ステップS303で復号化したコンテンツ鍵Kcon1, Kcon2, (Kcon3)の中のコンテンツ鍵Kcon1のみを相互認証の際に共有しておいたセッション鍵Ksesで暗号化する。【0454】記録再生器300の制御部302から読み出し、これらのデータを記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。【0455】次に、ステップS305において、記録再生器300から送信してきたコンテンツ鍵Kcon1を受信した記録デバイス400は、受信したコンテンツ鍵Kcon1を記録デバイス暗号処理部401の暗号/復号化部406に、相互認証の際に共有しておいたセッション鍵Ksesで復号化する。さらに、ステップS306において、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵Kstrで再暗号化させて、通信部404を介して記録再生器300に送信する。【0456】次に、ステップS307において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308において、ステップS303で復号化したコンテンツ鍵Kcon1, Kcon2, (Kcon3)の中のコンテンツ鍵Kcon2のみを相互認証の際に共有しておいたセッション鍵Ksesで暗号化する。【0457】記録再生器300から送信してきたコンテンツ鍵Kcon2を受信した記録デバイス400は、受信したコンテンツ鍵Kcon2を記録デバイス暗号処理部401の暗号/復号化部406に、相互認証の際に共有しておいたセッション鍵Ksesで復号化する。さらに、ステップS309において、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵Kstrで再暗号化させて、通信部404を介して記録再生器300に送信する。【0458】次に、ステップS310において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308において、ステップS303で復号化したコンテンツ鍵Kcon1, Kcon2, (Kcon3)の中のコンテンツ鍵Kcon3のみを相互認証の際に共有しておいたセッション鍵Ksesで暗号化する。【0459】記録再生器300の制御部302から読み出し、これらのデータを記録再生器300の記録デバイス暗号処理部302から読み出し、これらのデータを記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。【0460】次に、ステップS311において、記録再生器300から送信してきたコンテンツ鍵Kcon3を受信した記録デバイス400は、受信したコンテンツ鍵Kcon3を記録デバイス暗号処理部401の暗号/復号化部406に、相互認証の際に共有しておいたセッション鍵Ksesで復号化する。さらに、ステップS312において、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵Kstrで再暗号化させて、通信部404を介して記録再生器300に送信する。【0461】次に、ステップS313において、記録再生器の暗号処理部は、図32～35で説明した各種のデータフォーマットを形成して、記録デバイス400に送信する。【0462】最後にステップS314において、記録デバイス400は、フォーマット形成が終了した受信データを外部メモリ402に格納する。このフォーマットデータには、保存鍵Kstrで暗号化されたコンテンツ鍵Kcon1, Kcon2, (Kcon3)を含んでいる。【0463】このような処理を実行することにより、記録デバイス400に格納するコンテンツ鍵をトリプルDES方式の暗号方式による鍵として格納することが可能となる。なお、コンテンツ鍵がKcon1, Kcon2

の2つの鍵である場合は、ステップS310～S312の処理は省略される。【0464】このように、記録デバイスの構成、すなわちステップS305、S306の処理ステップを複数回、その対象を変更するのみで繰り返し実行することにより、トリプルDESの適用された鍵をメモリに格納可能となる。コンテンツ鍵KconがシングルDESの適用鍵である場合は、ステップS305、S306を実行して、ステップS313のフォーマット化処理を実行してメモリに格納すればよい。このような構成は、ステップS305、S306の処理を実行するコマンドを先に説明した図29のコマンドレジスターに格納し、この処理をコンテンツ鍵の構成、すなわちトリプルDES方式か、シングルDES方式かによって、適宜1回～3回実行する構成とすればよい。従って、記録デバイス400の処理ロジック中にトリプルDESの処理方式を含めることなく、トリプルDES方式、シングルDES方式、の双方の処理が可能となる。なお、暗号化方式については、コンテンツデータのヘッダ部内の取扱方針に記録し、これを参照することで判定することが可能である。【0465】(14)コンテンツデータ針中の起動優先順位に基づくプログラム起動処理先に説明されるように、本発明のデータ処理装置において利用されるコンテンツデータのヘッダ部に格納された取扱方針には、コンテンツタイプ、起動優先順位情報が含まれる。本発明のデータ処理装置における記録再生器300は、記録デバイス400、あるいは、DVD、CD、ハードディスク、さらにはゲームカートリッジ等の各種記録媒体に記録されたアクセス可能なコンテンツデータが複数存在する場合、これらコンテンツの起動順位を起動優先順位情報に従って決定する。【0466】記録再生器300は、記録デバイス400からコンテンツデータを再生、実行する場合の処理を中心として説明した。しかし、一般に記録再生器300は、図2に示すように記録デバイス400の他に、読み取り部304を介してDVD、CD、ハードディスク、さらに、PIO111、SIO112を介して接続されるメモリカード、ゲームカートリッジ等、各種記録媒体にアクセス可能な構成を有する。なお、図2で

は、図の複雑化を避けるため読み取り部304を1つの記録デバイスに記載しているが、記録再生器300は、異なる記憶媒体、例えばDVD、CD、フロッピーディスク、ハードディスクを並列に装着可能である。【0468】記録再生器300は、複数の記憶媒体にアクセス可能であり、それぞれの記憶媒体にはそれぞれコンテンツデータが格納されている。例えばCD等外部のコンテンツプロバイダが供給するコンテンツデータは、前述の図4のデータ構成でメディアに格納され、これらのメディアまたは、通信手段を介してダウンロードした場合には、図26、図27のコンテンツデータ構成でメモリカード等の各記憶媒体に格納されている。さらに、具体的には、コンテンツデータのフォーマットタイプに応じて図32～35に示すようにメディア上、記録デバイス上でそれぞれ異なるフォーマットで格納される。しかし、いずれの場合にもコンテンツデータのヘッダ中の取扱方針にはコンテンツタイプ、起動優先順位情報が含まれる。【0469】これら、複数のコンテンツデータに対するアクセスが可能な場合の記録再生器のコンテンツ起動処理をフローに従って説明する。【0470】図57は、起動可能な場合の処理例(1)を示す処理フローである。ステップS611は、記録再生器300がアクセス可能な記録デバイスの認証処理を実行するステップである。アクセス可能な記録デバイスには、メモリカード、DVD装置、CDドライブ、ハードディスク装置、さらに、例えばPIO111、SIO112を介して接続されるゲームカートリッジ等が含まれる。認証処理は、図2で示す制御部301の制御のもとに各記録デバイスに対して例えば先に図20で説明した手順に従って実行される。【0471】次に、記録デバイス内のメモリに格納されたコンテンツデータから起動可能なプログラムを検出する。これは、具体的には、コンテンツデータの取扱方針に含まれるコンテンツタイプがプログラムであるものを抽出する処理として実行される。【0472】次に、ステップS613において、S612で抽出された起動可能なプログラムにおける起動優先順位を判定する。これは、具体的には、ステップS612において選択された複数の起動可能なコンテンツデータのヘッダ中の取扱情報に含まれる優先情報を比較して最も高い優先順位を選択する処理である。【0473】プログラムを起動する。なお、複数の起動可能なプログラムにおいて設定された優先順位が同じである場合には、記録デバイス間でデフォルトの優先順位を設定し、最優先されるデバイスに格納されたコンテンツプログラムを実行する。【0474】図58には、複数の記録デバイスに識別子

を設定し、各識別子の付された記録デバイスについて順次、認証処理、コンテンツプログラム検索を実行する処理態様、すなわち起動可能コンテンツが複数ある場合の処理例（2）を示した。【0475】ステップS621では、に装着された記録デバイス（i）の認証処理（図20参照）を実行するステップである。複数（n個）の記録デバイスには順次1～nの識別子が付与されている。【0476】での認証が成功したか否かを判定し、認証が成功した場合は、ステップS623に進み、その記録デバイス（i）の記録媒体中から起動可能プログラムを検索する。認証が成功しなかった場合は、ステップS627に進み、新たにコンテンツ検索可能な記録デバイスの有無を判定し、無い場合は処理を終了し、記録デバイスが存在する場合は、ステップS628に進み記録デバイス識別子iを更新し、ステップS621以降の認証処理ステップを繰り返す。【0477】ステップS623における処理は、記録デバイス（i）に格納されたコンテンツデータから起動可能なプログラムを検出する処理である。これは、具体的には、コンテンツデータの取扱方針に含まれるコンテンツタイプがプログラムであるものを抽出する処理として実行される。【0478】ステップS624では、コンテンツがプログラムであるものが抽出されたか否かを判定し、抽出された場合は、ステップS625において、抽出プログラム中最も優先順位の高いものを選択し、ステップS626において選択プログラムを実行する。【0479】タイプがプログラムであるものが抽出されなかつたと判定された場合には、ステップS627に進み、新たにコンテンツ検索な記録デバイスの有無を判定し、無い場合は処理を終了し、記録デバイスが存在する場合は、ステップS628に進み記録デバイス識別子iを更新し、ステップS621以降の認証処理ステップを繰り返す。【0480】場合の処理例（3）を示す処理フローである。ステップS651は、記録再生器300がアクセス可能な記録デバイスの認証処理を実行するステップである。アクセス可能なDVD装置、CDドライブ、ハードディスク装置、メモリカード、ゲームカートリッジ等の認証処理を実行する。認証処理は、図2で示す制御部301の制御のもとに各記録デバイスに対して例えば先に図20で説明した手順に従って実行される。【0481】次に、ステップS652で抽出された起動可能なプログラムの名称等の情報を表示手段に表示する。なお、表示手段は図2では示されていないが、AV出力データとして出力されたデータが図示しない表示手段に出力される構成となっている。なお、各コンテンツデータのプログラム名等のユーザ提供情報は、コンテンツデータの識別情報中に格納されており、図2に示すメインCPU106の制御のもとに制御部301を介して認証済みの各コンテンツデータのプログラム名称等、プログラム情報を出力手段に出力する。【0483】次にステップS654では、図2に示す入力インターフェース、コントローラ、マウス、キーボード等の入力手段からのユーザによるプログラム選択入力を入力インターフェース110を介してメインCPU106が受領し、選択入力をしたがって、ステップS655においてユーザ選択プログラムを実行する。【0484】このようにコンテンツデータ中のヘッダ内の取扱情報にプログラム起動優先順位情報を格納し、記録再生器300がこの優先順位に従ってプログラムを起動する、あるいは表示手段に起動プログラム情報を表示してユーザによって選択する構成としたので、ユーザがプログラムを検索する必要がなく、起動に要する時間およびユーザの労力を省くことが可能となる。また、起動可能なプログラムは、すべて記録デバイスの認証処理後に起動、または起動可能プログラムであることの表示がなされるので、プログラムを選択してから正当性の確認を行なう等の処理の煩雑性が解消される。【0485】（15）コンテンツ構成および再生長）処理本発明のデータ処理装置では、上述のように記録再生器300は、メディア500または通信手段600からコンテンツをダウンロード、あるいは記録デバイス400から再生処理を行う。上記の説明は、コンテンツのダウンロード、あるいは再生処理に伴う、暗号化データの処理を中心として説明してきた。【0486】図3の記録再生器301は、コンテンツデータを提供するDVD等のデバイス500、通信手段600、記録デバイスからのコンテンツデータのダウンロード処理、または再生処理に伴う認証処理、暗号化、復号化処理全般を制御する。【0487】このようなコンテンツは、例えば音声データ、画像データ等である。復号データは制御部301から図2に示すメインCPUの制御下に置かれ、音声データ、画像データ等に応じてAV出力部に出力される。しかし、コンテンツが例えば音声データであってMP3圧縮がなされていれば、図2に示すAV出力部のMP3デコーダによって音声デ

として実行される。【0482】次に、ステップS653においてステップS652で抽出された起動可能なプログラムの名称等の情報を表示手段に表示する。なお、表示手段は図2では示されていないが、AV出力データとして出力されたデータが図示しない表示手段に出力される構成となっている。なお、各コンテンツデータのプログラム名等のユーザ提供情報は、コンテンツデータの識別情報中に格納されており、図2に示すメインCPU106の制御のもとに制御部301を介して認証済みの各コンテンツデータのプログラム名称等、プログラム情報を出力手段に出力する。【0483】次にステップS654では、図2に示す入力インターフェース、コントローラ、マウス、キーボード等の入力手段からのユーザによるプログラム選択入力を入力インターフェース110を介してメインCPU106が受領し、選択入力をしたがって、ステップS655においてユーザ選択プログラムを実行する。【0484】このようにコンテンツデータ中のヘッダ内の取扱情報にプログラム起動優先順位情報を格納し、記録再生器300がこの優先順位に従ってプログラムを起動する、あるいは表示手段に起動プログラム情報を表示してユーザによって選択する構成としたので、ユーザがプログラムを検索する必要がなく、起動に要する時間およびユーザの労力を省くことが可能となる。また、起動可能なプログラムは、すべて記録デバイスの認証処理後に起動、または起動可能プログラムであることの表示がなされるので、プログラムを選択してから正当性の確認を行なう等の処理の煩雑性が解消される。【0485】（15）コンテンツ構成および再生長）処理本発明のデータ処理装置では、上述のように記録再生器300は、メディア500または通信手段600からコンテンツをダウンロード、あるいは記録デバイス400から再生処理を行う。上記の説明は、コンテンツのダウンロード、あるいは再生処理に伴う、暗号化データの処理を中心として説明してきた。【0486】図3の記録再生器301は、コンテンツデータを提供するDVD等のデバイス500、通信手段600、記録デバイスからのコンテンツデータのダウンロード処理、または再生処理に伴う認証処理、暗号化、復号化処理全般を制御する。【0487】このようなコンテンツは、例えば音声データ、画像データ等である。復号データは制御部301から図2に示すメインCPUの制御下に置かれ、音声データ、画像データ等に応じてAV出力部に出力される。しかし、コンテンツが例えば音声データであってMP3圧縮がなされていれば、図2に示すAV出力部のMP3デコーダによって音声デ

ータの復号処理がなされて出力される。また、コンテンツデータが画像データであり、MPEG 2圧縮画像であれば、AV処理部のMPEG 2デコーダによって伸長処理が実行されて出力されることになる。このように、コンテンツデータに含まれるデータは、圧縮（符号化）処理がなされている場合もあり、また圧縮処理の施されていないデータもあり、コンテンツに応じた処理を施して出力する。【0488】しかしながら、圧縮処理、伸長処理プログラムには、様々な種類があり、コンテンツプロバイダから圧縮データを提供されても対応する伸長処理実行プログラムが無い場合は、これを再生することができないという事態が発生する。【0489】そこで、本発明のデータ処理中に、圧縮データとその復号（伸長）処理プログラムを併せて格納する構成、あるいは圧縮データと復号（伸長）処理プログラムとのリンク情報をコンテンツデータのヘッダ情報として格納する構成を開示する。【0490】図2に示したデータ処理全体図から、本構成に関する要素および関連要素を簡潔にまとめた図を図60に示す。記録再生器300は、例えばDVD、CD等のデバイス500、または通信手段600、あるいはコンテンツを格納したメモリカード等の記録デバイス400から様々なコンテンツの提供を受ける。これらのコンテンツは、音声データ、静止画像、動画像データ、プログラムデータ等であり、また暗号化処理の施されているもの、施されていないもの、また、圧縮処理がなされているもの、なされていないもの等、様々なデータが含まれる。【0491】受領コンテンツが暗号化されている場合は、すでに上述した項目中で説明したような手法によって制御部301の制御、および暗号処理部302の暗号処理によって復号処理が実行される。復号されたデータはメインCPU106の制御下で、AV処理部に109に転送され、AV処理部109のメモリ3090に格納された後、コンテンツ解析部3091においてコンテンツ構成の解析が実行される。例えばコンテンツ中にデータ伸長プログラムが格納されていれば、プログラム記憶部3093にプログラムを格納し、音声データ、画像データ等のデータが含まれていればこれらをデータ記憶部3092に記憶する。伸長処理部3094では、プログラム記憶部に記憶された例えばMP3等の伸長処理プログラムを用いてデータ記憶部3092に記憶された圧縮データの伸長処理を実行して、スピーカ3001、モニタ3002に出力される。【0492】次に、AV処理部109に介して受領するデータの構成および処理のいくつかの例について説明する。なお、ここでは、コンテンツの例として音声データを示し、また圧縮プログラムの例として

MP3を適用したものを代表して説明するが、本構成は、音声データのみならず、画像データにも適用できるものであり、また、圧縮伸長処理プログラムについてもMP3のみならず、MPEG2、4等各種のプログラムを適用することが可能である。【0493】図61にコンテンツ構成部はMP3によって圧縮された音楽データ6102、MP3復号（伸長）処理プログラム6101を併せて1つのコンテンツとして構成した例である。これらのコンテンツは、1コンテンツとしてメディア500、あるいは記録デバイス400に格納され、または通信手段600から配信される。記録再生器300は、これらのコンテンツは、暗号処理部303によって復号処理を実行した後、AV処理部109に転送される。【0494】AV処理部109の91では、受け取ったコンテンツを解析し、音声データ伸長プログラム（MP3デコーダ）部と、圧縮音声データ部からなるコンテンツから、音声データ伸長プログラム（MP3デコーダ）部を取り出してプログラム記憶部3093にプログラムを記憶し、圧縮音声データをデータ記憶部3092に記憶する。なお、コンテンツ解析部3091は、コンテンツとは別に受領したコンテンツ名、コンテンツ構成情報等の情報を受領したり、あるいはコンテンツ内に含まれるデータ名等の識別データ、データ長、データ構成等を示すデータに基づいてコンテンツ解析を実行してもよい。次に、圧縮伸長処理部3094は、プログラム記憶部3093に記憶された音声データ伸長プログラム（MP3デコーダ）に従ってデータ記憶部3092に記憶されたMP3圧縮音声データの伸長処理を実行して、AV処理部109は伸長した音声データをスピーカ3001に出力する。【0495】図62に図61のデータの再生処理の一例を示すフローを示す。ステップS671は、AV処理部109のメモリ3090に格納されたデータ名、例えば音楽データのコンテンツであれば曲名等の情報をコンテンツとは別に受領した情報、あるいはコンテンツ内のデータから取り出し、モニタ3002に表示する。ステップS672は、ユーザの選択をスイッチ、キーボード等の各種入力手段から入力インターフェース110を介して受領し、CPU106の制御のもとにユーザ入力データに基づく再生処理命令をAV処理部109に出力する。AV処理部109は、ステップS673においてユーザ選択によるデータの抽出、伸長処理を実行する。【0496】次に図63に、1つのコンテンツには音声データ、あるいは伸長処理プログラムのいずれか一方が含まれ、さらに各コンテンツのヘッダ情報としてコンテンツの内容を示すコンテンツ情報が含まれる構成例を示す。

【0497】図63に示すように、コンテンツがプログラム6202である場合は、ヘッダ情報6201としてプログラムであること、およびプログラム種類がMP3伸長プログラムであることを示すコンテンツ識別情報が含まれる。一方、音声データ6204をコンテンツとして含む場合は、ヘッダ6203のコンテンツ情報にはMP3圧縮データであるとの情報が含まれる。このヘッダ情報は、前述した例えは図4に示すコンテンツデータ構成の取扱方針（図5参照）中に含まれるデータから再生に必要な情報のみを選択してAV処理部109へ転送するコンテンツに付加して構成することが可能である。具体的には、図5に示す「取扱方針」中の各構成データに暗号処理部302において必要となる取扱方針データと、AV処理部109における再生処理時に必要となるデータとの識別値を付加し、これら識別値が、AV処理部109において必要であることを示すもののみを抽出してヘッダ情報とすることができます。【0498】図63に示す再生処理部109のコンテンツ解析部3091は、ヘッダ情報に従って、プログラムである場合はプログラムコンテンツをプログラム記憶部3093に記憶し、データである場合は、データコンテンツをデータ記憶部3092に記憶する。その後、圧縮伸長処理部3094は、データ記憶部からデータを取り出して、プログラム記憶部3093に記憶したMP3プログラムに従って伸長処理を実行して出力する。なお、プログラム記憶部3093にすでに同一プログラムが格納されている場合は、プログラム格納処理は省略してもよい。【0499】図64に図63のデータの再生処理の一例を示すフローを示す。ステップS675は、AV処理部109のメモリ3090に格納されたデータ名、例えば音楽データのコンテンツであれば曲名等の情報をコンテンツとは別に受領した情報、あるいはコンテンツ内のヘッダから取り出し、モニタ3002に表示する。ステップS676は、ユーザの選択をスイッチ、キーボード等の各種入力手段から入力インターフェース110を介して受領する。【0500】次に、ステップに対応するデータの再生用プログラム（例えばMP3）を検索する。このプログラム検索対象は、記録再生機器300のアクセス可能な範囲を最大検索範囲とすることが好ましく、例えば図60に示す、各メディア500、通信手段600、記録デバイス400等も検索範囲とする。【0501】AV処理部109に渡されるコンテンツはデータ部のみであり、プログラムコンテンツは記録再生器300内の他の記録媒体に格納される場合もあり、DVD、CD等のメディアを介してコンテンツ提供業者から提供されることもある。従って、検索対象を記録再生機器300のアクセス格納範囲を検索範囲とする。検

索の結果として再生プログラムが見つかると、CPU106の制御のもとにユーザ入力データに基づく再生処理命令をAV処理部109に出力する。AV処理部109は、ステップS679においてユーザ選択によるデータの抽出、伸長処理を実行する。また、別の実施例として、プログラムの検索をステップS675より前に行い、ステップS675においては、プログラムが検出されたデータのみを表示するようにしてもよい。【0502】次に音声データ6303、伸長処理プログラム6302が含まれ、さらにコンテンツのヘッダ情報6301としてコンテンツの再生優先順位情報が含まれる構成例を示す。これは、先の図61のコンテンツ構成にヘッダ情報として再生優先順位情報を付加した例である。これは、前述の「（14）コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理」と同様、AV処理部109が受領したコンテンツ間において設定されたデータの再生順位に基づいて再生順を決定するものである。【0503】図63に示す再生処理の一例を示すフローを示す。ステップS681は、AV処理部109のメモリ3090に格納されたデータ、すなわち再生対象データのデータ情報を検索リストに設定する。検索リストはAV処理部109内のメモリの一部領域を使用して設定する。次に、ステップS682において、AV処理部109のコンテンツ解析部3091において検索リストから優先順位の高いデータを選択し、ステップS683において、選択されたデータの再生処理を実行する。【0504】次に図67に、1つデータの再生処理の一例を示すフローを示す。ステップS681は、AV処理部109のメモリ3090に格納されたデータ、すなわち再生対象データのデータ情報を検索リストに設定する。検索リストはAV処理部109内のメモリの一部領域を使用して設定する。次に、ステップS682において、AV処理部109のコンテンツ解析部3091において検索リストから優先順位の高いデータを選択する。【0505】図68に図67のコンテンツ構成を持つデータの再生処理の一例を示すフローを示す。ステップS691は、AV処理部109のメモリ3090に格納されたデータ、すなわち再生対象データのデータ情報を検索リストに設定する。検索リストはAV処理部109内のメモリの一部領域を使用して設定する。次に、ステップS692において、AV処理部109のコンテンツ解析部3091において検索リストから優先順位の高いデータを選択する。【0506】次に、ステップS693では、選択データに対応するデータ再生用プログラム（例えばMP3）を検索する。このプログラム検索対象は、先の図64のフローにおける処理と同様、記録再生機器300のアクセス格納範囲を最大検索範囲とすることが好ましく、例えば図60に示す各メディア500、通信手段600、記録デバイス400等も検索範囲とする。

【0507】検索の結果として再生プログラムが見つかる（ステップS694でYes）と、ステップS695において、選択されたデータを検索の結果得られたプログラムを用いて、伸長再生処理を実行する。【0508】それなかった場合（ステップS694でNo）は、ステップS696に進み、ステップS691で設定した検索リスト中に含まれる他のデータにおいて、同一のプログラムを用いた再生処理が必要なものを削除する。これは、新たにそのデータに対する再生プログラム検索を実行しても検出されないことが明らかであるからである。さらに、ステップS697において検索リストが空であるかを判定し、からでない場合は、ステップS692に戻り、さらに次の優先順位の高いデータを抽出して、プログラム検索処理を実行する。【0509】このように、されたコンテンツは、その復号（伸長）プログラムと共に構成されるか、あるいはコンテンツが圧縮されたデータのみ、あるいは伸長処理プログラムのみである場合は、それぞれのコンテンツにコンテンツがどのような圧縮データであるのか、あるいはどのような処理を実行するかを示すヘッダ情報を有しているので、コンテンツを受領した処理部（例えばAV処理部）は、圧縮データに付属する伸長処理プログラムを用いて伸長再生処理を実行するか、あるいは伸長処理プログラムを圧縮データのヘッダ情報に基づいて検索して、検索の結果得られたプログラムにしたがって伸長再生処理を実行するので、ユーザによるデータの伸長プログラムの選択、検索等の処理が不要となりユーザ負担が軽減され、効率的なデータ再生が可能となる。さらに、ヘッダに再生優先順位情報を有した構成によれば、再生順序を自動設定する構成が可能となり、ユーザによる再生順設定の操作を省略することができる。【0510】なお、上述の実施例では、圧縮音声データ、コンテンツ、および音声圧縮データの伸長処理プログラムとしてのMP3を例として説明したが、圧縮データを含むコンテンツ、圧縮画像データの伸長処理プログラムを有するコンテンツであっても本構成は同様に適用可能であり、同様の効果を奏するものである。【0511】バイスへの格納、再生処理本発明のデータ処理装置は、例において実行されるコンテンツがゲームプログラム等である場合等、ゲームプログラムを途中で中断して、所定時間後、新たに再開したい場合には、その中断時点のゲーム状態等をセーブ、すなわち記録デバイスに格納し、これを再開時に読み出してゲームを続行することが可能な構成を持つ。【0512】従来のゲーム機器、パソコン等の機器におけるセーブデータ保存構成は、例えば記録再生器

に内蔵、あるいは外付け可能なメモリカード、フロッピーディスク、ゲームカートリッジ、あるいはハードディスク等の記憶媒体にセーブデータを保存する構成を持つ一方が、特に、そのセーブデータに対するセキュリティ確保構成を有しておらず、例えばゲームアプリケーションプログラムに共通の仕様でデータのセーブ処理が行われる構成となっている。【0513】従って、例えばある1つの記録用いてセーブされたセーブデータが別のゲームプログラムによって使用されたり、書換えられたりする事態が発生し、従来、セーブデータのセキュリティはほとんど考慮されていなかったのが実状である。【0514】本発明のデーターブデータのセキュリティ確保を実現可能とした構成を提供する。例えばあるゲームプログラムのセーブデータ本構成は、そのゲームプログラムのみが使用可能な情報に基づいて暗号化して記録デバイスに格納する。あるいは、記録再生器固有の情報に基づいて暗号化して記録デバイスに格納する。これらの手法により、セーブデータの利用を特定の機器、特定のプログラムのみに制限することができ、セーブデータのセキュリティが確保される。以下、本発明のデータ処理装置における「セーブデータの生成および記録デバイスへの格納、再生処理」について説明する。【0515】図69に本発明のデータ処理装置におけるセーブデータ格納処理について説明するブロック図を示す。DVD、CD等のメディア500、あるいは通信手段600からコンテンツが記録再生器300に提供される。提供されるコンテンツは、先に説明したようにコンテンツ固有の鍵であるコンテンツ鍵Kconによって暗号化されており、記録再生器300は、前述した「（7）記録再生器から記録デバイスへのダウンロード処理」の欄で説明（図22参照）した処理に従ってコンテンツ鍵を取得して、暗号化コンテンツを復号した後、記録デバイス400に格納する。ここでは、記録再生器300がコンテンツプログラムをメディア、通信手段から復号して再生、実行を行ない、実行の後、得られるセーブデータを外付け、あるいは内蔵のメモリカード、ハードディスク等の各種の記録デバイス400A、400B、400Cのいずれかに格納し、再生する処理、あるいはコンテンツを記録デバイス400Aにダウンロードした後、記録デバイス400Aからコンテンツを再生、実行して、そのセーブデータを外付け、あるいは内蔵のメモリカード、ハードディスク等の各種の記録デバイス400A、400B、400Cのいずれかに格納する処理記録デバイス400に格納し、再生する処理について説明する。【0516】記録再生器300には、先に説明したように記録再生器識別子IDdev、システムに共通な署名鍵であるシステム署名鍵Ksys、個々の記録再生器に

固有の署名鍵である記録再生器署名鍵K_{d e v}、さらに各種の個別鍵を生成するマスタ鍵を有する。マスタ鍵について、「(12) マスタ鍵に基づく暗号処理鍵生成構成」において、詳しく説明した通り、例えば、配送鍵K_{d i s}、あるいは認証鍵K_{a k e}等を生成する鍵である。ここでは、特にマスタ鍵の種類を限定することなく記録再生器300の有するマスタ鍵全般を代表するものとしてMK_xとして示す。図69の下段には、セーブデータの暗号鍵K_{s a v}の例を示した。セーブデータ暗号鍵K_{s a v}は、セーブデータを各種記録デバイス400A～Cに格納する場合の暗号化処理、そして、各種記録デバイス400A～Cから再生する際の復号処理に用いられる暗号鍵である。図70以下を用いて、セーブデータの格納処理および再生処理の例を説明する。【0517】通鍵のいずれかを用いてセーブデータを記録デバイス400A～Cいずれかに格納する処理のフロー図である。なお、各フローにおける処理は記録再生器300が実行する処理であり、各フローでセーブデータを格納する記録デバイスは内蔵、外付け記録デバイス400A～Cのいずれかであればよく、いずれかに限定するものではない。【0518】ステップS701は、コンテンツ識別子、例えばゲームIDを記録再生器300が読み出す処理である。これは、先に説明した図4、26、27、32～35に示すコンテンツデータ中の識別情報に含まれるデータであり、セーブデータの格納処理命令を図2に示す入力インタフェース110を介して受領したメインCPU106がコンテンツ識別子の読み取りを制御部301に指示する。【0519】制御部301は、実行プログラムがD、CD-ROM等、読み取部304を介して実行されているコンテンツの場合は、読み取部304を介してコンテンツデータ中のヘッダに含まれる識別情報を取り出し、実行プログラムが、記録デバイス400に格納されたコンテンツである場合は、記録デバイスコントローラ303を介して識別情報を取り出す。なお、記録再生器300がコンテンツプログラムを実行中で、すでに記録再生器中のRAM、その他のアクセス可能な記録媒体にコンテンツ識別子が格納済みである場合は、新たな読み取り処理を実行せずに、読み込み済みデータに含まれる識別情報を利用してもよい。【0520】次に、ステップS702使用制限を行なうか否かによって処理を変更するステップである。プログラム使用制限とは、保存するセーブデータをそのプログラムのみに固有に利用可能とする制限を付するか否かを設定する制限情報であり、プログラムのみに固有に利用可能とする場合は、「プログラム使用制限あり」とし、プログラムに利用を拘束されないセーブデータとする場合を「プログラム使用制限なし」とす

る。これは、ユーザが任意に設定できるようにしてもよいし、コンテンツ製作者が設定して、この情報をコンテンツプログラム中に格納しておいてもよく、設定された制限情報は、図69の記録デバイス400A～Cにデータ管理ファイルとして格納される。【0521】データ管理ファイルは項目としてデータ番号、コンテンツ識別子、記録再生器識別子、プログラム使用制限を含むテーブルとして生成される。コンテンツ識別子は、セーブデータを格納する対象となったコンテンツプログラムの識別データである。記録再生器識別子は、セーブデータを格納した記録再生器の識別子、例えば図69に示す【ID_{d e v}】である。プログラム使用制限は、上述したように保存するセーブデータをそのプログラムのみに固有に利用可能とす場合、「する」の設定とし、対応プログラムに制限されない利用を可能とする場合「しない」の設定となる。プログラム使用制限は、コンテンツプログラムを利用するユーザが任意に設定できるようにしてもよいし、コンテンツ製作者が設定して、この情報をコンテンツプログラム中に格納しておいてもよい。【0522】ステップS702において、プログラム使用制限について「する」の設定がされている場合は、ステップS703に進む。ステップS703では、コンテンツデータからコンテンツ固有の鍵、例えば先に説明したコンテンツ鍵K_{c o n}を読み出してコンテンツ固有鍵をセーブデータ暗号鍵K_{s a v}とするか、あるいはコンテンツ固有鍵に基づいてセーブデータ暗号鍵K_{s a v}を生成する。【0523】ラム使用制限について「しない」の設定がされている場合は、ステップS707に進む。ステップS707では、記録再生器300内に格納されたシステム共通鍵、例えばシステム署名鍵K_{s y s}を記録再生器300の内部メモリ307から読み出して、システム署名鍵K_{s y s}をセーブデータ暗号鍵K_{s a v}とするか、あるいはシステム署名鍵に基づいてセーブデータ暗号鍵K_{s a v}を生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K_{s a v}として使用してもよい。【0524】ステップS703、またはステップS707で選択、または生成されたセーブデータ暗号化鍵K_{s a v}を用いてセーブデータの暗号化処理を実行する。この暗号化処理は、図2における暗号処理部302が例えば前述のDESアルゴリズムを適用して実行する。【0525】ステップS704にまたセーブデータは、ステップS705において記録デバイスに格納される。セーブデータを格納可能な記録デバイスが図69に示すように複数ある場合は、ユーザが記録デバイス400A～Cのいずれかをセーブデータ格納

先として予め選択する。さらに、ステップS706において先に図71を用いて説明したデータ管理ファイルに先にステップS702で設定したプログラム使用制限情報の書き込み、すなわちプログラム使用制限「する」または「しない」の書き込みを実行する。【0526】以上で、ステップS702においてY e s、すなわち「プログラム使用制限する」の選択がなされ、ステップS703においてコンテンツ固有鍵に基づいて生成されたセーブデータ暗号化鍵Ks a vによって暗号化処理されたセーブデータは、コンテンツ固有鍵情報を持たないコンテンツプログラムによる復号処理が不可能となり、セーブデータは同じコンテンツ鍵情報を有するコンテンツプログラムのみが利用できることになる。ただし、ここでは、セーブデータ暗号化鍵Ks a vは記録再生器固有の情報に基いて生成されたものではないので、例えばメモリカード等の着脱可能な記録デバイスに格納されたセーブデータは異なる記録再生器においても対応するコンテンツプログラムと共に使用する限り再生可能となる。【0527】なわち「プログラム使用制限しない」の選択がなされ、ステップS707においてシステム共通鍵に基づくセーブデータ暗号化鍵Ks a vによって暗号化処理されたセーブデータは、コンテンツ識別子が異なるプログラムを用いた場合でも、また、記録再生器が異なっていた場合でも再生して利用することが可能となる。【0528】図72によって格納されたセーブデータを再生する処理を示したフローである。【0529】ステップS711は、コンテンツデータ中の識別情報に含まれるデータを読み出す処理である。これは、先に説明した図70のセーブデータ格納処理のステップS701と同様の処理であり、コンテンツデータ中の識別情報に含まれるデータを読み出す処理である。【0530】次に、ステップS712では、図69に示す記録デバイス400A～Cから、図71を用いて説明したデータ管理ファイルを読み出し、ステップS711において読み出したコンテンツ識別子、および対応して設定された使用プログラム制限情報を抽出する。データ管理ファイルに設定されたプログラム使用制限が「する」であった場合は、ステップS714に進み、「しない」であった場合には、ステップS717に進む。【0531】からコンテンツ固有の鍵、例えば先に説明したコンテンツ鍵Kc o nを読み出してコンテンツ固有鍵をセーブデータ復号化鍵Ks a vとするか、あるいはコンテンツ固有鍵に基づいてセーブデータ復号化鍵Ks a vを生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、あるコンテンツ固有

鍵に基づいて暗号化されたデータは、同一のコンテンツ固有鍵に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。【0532】管理ファイルの設定がプログラム使用制限について「しない」の設定であった場合は、ステップS717において、記録再生器300内に格納されたシステム共通鍵、例えばシステム署名鍵Ks y sを記録再生器300の内部メモリ307から読み出して、システム署名鍵Ks y sをセーブデータ復号化鍵Ks a vとするか、あるいはシステム署名鍵に基づいてセーブデータ復号化鍵Ks a vを生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵Ks a vとして使用してもよい。【0533】次に、ステップS715において、ステップS714、またはステップS717で選択、または生成されたセーブデータ復号化鍵Ks a vを用いてセーブデータの復号化処理を実行し、ステップS716において復号したセーブデータを記録再生器300において再生、実行する。【0534】以上で、セーブデータの再生処理が、上述のようにデータ管理ファイルに「プログラム使用制限する」の設定がなされている場合は、コンテンツ固有鍵に基づいてセーブデータ復号化鍵が生成され、「プログラム使用制限しない」の設定がある場合はシステム共通鍵に基づいてセーブデータ復号化鍵が生成される。「プログラム使用制限する」の設定がされている場合、使用しているコンテンツのコンテンツ識別子が同じものでないとセーブデータの復号処理の可能な復号化鍵を得ることができないこととなり、セーブデータのセキュリティを高めることができるとなる。【0535】図73、図74においてセーブデータの暗号化鍵、復号化鍵を生成するセーブデータ格納処理フロー（図73）、セーブデータ再生処理フロー（図74）である。【0536】図73において、ステップS701～S702は、図70のステップS701～S702と同様の処理であり、説明を省略する。【0537】図73のセーブデータステップS722において「プログラム使用制限する」の設定を行なった場合、ステップS723においてコンテンツデータからコンテンツ識別子、すなわちコンテンツIDを読み出してコンテンツIDをセーブデータ暗号化鍵Ks a vとするか、あるいはコンテンツIDに基づいてセーブデータ暗号化鍵Ks a vを生成する。例えば、記録再生器300の暗号処理部307はコンテンツデータから読み出したコンテンツIDに、記録再生器300の内部メモリに格納されたマスター鍵MK xを適用して、例えばDES（MK x、コンテンツID）によつ

てセーブデータ暗号化鍵K_{s a v}を得ることができる。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵K_{s a v}として使用してもよい。【0538】一方、ステップS727において、記録再生器300内に格納されたシステム共通鍵、例えばシステム署名鍵K_{s y s}を記録再生器300の内部メモリ307から読み出して、システム署名鍵K_{s y s}をセーブデータ暗号化鍵K_{s a v}とするか、あるいはシステム署名鍵に基づいてセーブデータ暗号化鍵K_{s a v}を生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵K_{s a v}として使用してもよい。【0539】ステップS727の処理フローにおけるステップS704以下の処理と同様であり、説明を省略する。【0540】さらに、図74の処理フローで記録デバイスに格納されたセーブデータを再生、実行する処理フローであり、ステップS731～S733は前述の図72の対応処理と同様であり、ステップS734のみが異なる。ステップS734においては、コンテンツデータからコンテンツ識別子、すなわちコンテンツIDを読み出してコンテンツIDをセーブデータ復号化鍵K_{s a v}とするか、あるいはコンテンツIDに基づいてセーブデータ復号化鍵K_{s a v}を生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、あるコンテンツ識別子に基づいて暗号化されたデータは、同一のコンテンツ識別子に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。6、S737は、図72の対応処理と同様であるので説明を省略する。図73、図74のセーブデータ格納および再生処理に従えば、プログラム使用制限するの設定を行なった場合、コンテンツIDを使用してセーブデータ暗号化鍵、復号化鍵を生成する構成としたので、先のコンテンツ固有鍵を使用したセーブデータ格納、再生処理と同様、対応するコンテンツプログラムが整合する場合以外は、セーブデータを利用ることができない構成となり、セーブデータセキュリティを高めた保存が可能となる。【0542】図75、図77は、記録再生器固有鍵を用いてセーブデータの暗号化鍵、復号化鍵を生成するセーブデータ格納処理フロー(図75)、セーブデータ再生処理フロー(図77)である。【0543】図75において、ステップS701と同様の処理であり、説明を省略する。ステップS742は、記録再生器の制限をする

かしないかを設定するステップである。記録再生器制限は、セーブデータを利用可能な記録再生器を限定する場合、すなわちセーブデータを生成し格納した記録再生器にのみ利用可能とする場合を「する」と設定し、他の記録再生器でも利用可能とする場合を「しない」の設定とするものである。ステップS742において「記録再生器制限する」の設定をすると、ステップS743に進み、「しない」の設定をするとステップS747に進む。【0544】データ管理ファイルの例を図76に示す。データ管理ファイルは項目としてデータ番号、コンテンツ識別子、記録再生器識別子、記録再生器制限を含むテーブルとして生成される。コンテンツ識別子は、セーブデータを格納する対象となったコンテンツプログラムの識別データである。記録再生器識別子は、セーブデータを格納した記録再生器の識別子、例えば図69に示す【IDdev】である。記録再生器制限は、セーブデータを利用可能な記録再生器を限定する場合、すなわちセーブデータを生成し格納した記録再生器にのみ利用可能とする場合を「する」と設定し、他の記録再生器でも利用可能とする場合を「しない」の設定とするものである。記録再生器制限情報は、コンテンツプログラムを利用するユーザが任意に設定できるようにしてもよいし、コンテンツ製作者が設定して、この情報をコンテンツプログラム中に格納しておいてもよい。【0545】図75のセーブデータ格納においては、ステップS742において「記録再生器制限する」の設定を行なった場合、ステップS743において記録再生器300から記録再生器固有鍵、例えば記録再生器署名鍵K_{d e v}を記録再生器300の内部メモリ307から読み出して記録再生器署名鍵K_{d e v}をセーブデータ暗号化鍵K_{s a v}とするか、あるいは記録再生器署名鍵K_{d e v}に基づいてセーブデータ暗号化鍵K_{s a v}を生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵K_{s a v}として使用してもよい。【0546】一方、ステップS742において、記録再生器制限について「しない」の設定とした場合は、ステップS747において、記録再生器300内に格納されたシステム共通鍵、例えばシステム署名鍵K_{s y s}を記録再生器300の内部メモリ307から読み出して、システム署名鍵K_{s y s}をセーブデータ暗号化鍵K_{s a v}とするか、あるいはシステム署名鍵に基づいてセーブデータ暗号化鍵K_{s a v}を生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵K_{s a v}として使用してもよい。【0547】ステップS744、S7450の図70の処理フローにおける対応処理と同様であ

り、説明を省略する。【0548】ステップS746では、デ再生処理フローによれば、「記録再生器制限する」の選択がなされたセーブデータは、記録再生器固有鍵によって暗号化、復号化処理が実行されるため、同一の記録再生器制限情報「する／しない」を書き込む。【0549】さらに生器個有鍵を持つ記録再生器、すなわち同一の記録再生器によってのみ復号して利用することが可能となる。【0555】を用いてセーブデータの暗号化、復号化鍵を生成して格納、再生する処理フローを示す。【0556】図78は、記録再生データの暗号化を行い記録デバイスに格納する。ステップS761～S763は、先の図75と同様の処理である。ステップS764では、記録再生器から読み出した記録再生器識別子(IDdev)を用いてセーブデータの暗号化鍵Ksavを生成する。IDdevをセーブデータ暗号化鍵Ksavとして適用するか、あるいは記録再生器300の内部メモリに格納されたマスター鍵MKxを適用して、DES(MKx, IDdev)によってセーブデータ暗号化鍵Ksavを得る等、IDdevに基づいてセーブデータ暗号化鍵Ksavを生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ksavとして使用してもよい。【0557】以下の処理は、前述の図75の対応処理と同様であり、説明を省略する。【0558】図79は、図78の処理によって記録デバイスに格納されたセーブデータを再生、実行する処理フローである。ステップS771～S774は、前述の図77の対応処理と同様である。【0559】ステップS775で読み出した記録再生器識別子(IDdev)を用いてセーブデータの復号化鍵Ksavを生成する。IDdevをセーブデータ復号化鍵Ksavとして適用するか、あるいは記録再生器300の内部メモリに格納されたマスター鍵MKxを適用して、DES(MKx, IDdev)によってセーブデータ復号化鍵Ksavを得る等、IDdevに基づいてセーブデータ復号化鍵Ksavを生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、ある記録再生器固有鍵に基づいて暗号化されたデータは、同一の記録再生器固有鍵に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ksavとして使用してもよい。【0553】一方で、記録再生器300内に格納されたシステム共通鍵、例えばシステム署名鍵Ksysを記録再生器300の内部メモリ307から読み出して、システム署名鍵Ksysをセーブデータ復号化鍵Ksavとするか、あるいはシステム署名鍵に基づいてセーブデータ復号化鍵Ksavを生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ksavとして使用してもよい。以下のステップS756, S757は、前述のセーブデータ再生処理フローの対応ステップと同様の処理である。【0554】の選択がなされたセーブデータは、記録再生器識別子に

よって暗号化、復号化処理が実行されるため、同一の記録再生器識別子を持つ記録再生器、すなわち同一の記録再生器によってのみ復号して利用することが可能となる。【0562】次に図80～82を用いて、上述のプログラム使用制限、および記録再生器使用制限を併せて実行するセーブデータ格納、再生処理について説明する。【0563】において記録再生器制限判定を行なう。【0564】「再生器制限あり」の場合は、ステップS785において、コンテンツ固有鍵(ex. Kcon)と、記録再生器固有鍵(Kdev)の双方に基づいてセーブデータ暗号化鍵Ksavが生成される。これは、例えばKsav = (Kcon XOR Kdev)、あるいは記録再生器300の内部メモリに格納されたマスク鍵MKxを適用してKsav=DES(MKx, Kcon XOR Kdev)等によって得ることができる。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵Ksavとして使用してもよい。【0565】「プログラム使用制限なし」の場合は、ステップS786において、コンテンツ固有鍵(ex. Kcon)をセーブデータ暗号化鍵Ksavとするか、あるいはコンテンツ固有鍵(ex. Kcon)に基づいてセーブデータ暗号化鍵Ksavを生成する。【0566】「プログラム使用制限なし」の場合は、ステップS787において、記録再生器固有鍵(Kdev)をセーブデータ暗号化鍵Ksavとするか、あるいは記録再生器固有鍵(Kdev)に基づいてセーブデータ暗号化鍵Ksavが生成される。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵Ksavとして使用してもよい。【0567】「記録再生器制限なし」の場合は、ステップS787において、システム共通鍵、例えばシステム署名鍵Ksysをセーブデータ暗号化鍵Ksavとするか、あるいはシステム署名鍵Ksysに基づいてセーブデータ暗号化鍵Ksavを生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵Ksavとして使用してもよい。【0568】ステップS789では、ステップS～S788のいずれかで生成されたセーブデータ暗号化鍵Ksavによってセーブデータが暗号化され、記録デ

バイスに格納される。【0569】さらに、ステップS790でS782、S783において設定した制限情報がデータ管理ファイルに格納される。データ管理ファイルは、例えば図81に示す構成となり、項目としてデータ番号、コンテンツ識別子、記録再生器識別子、プログラム使用制限、記録再生器制限を含む。【0570】図82は、図80の例に格納されたセーブデータを再生、実行する処理フローである。ステップS791では、実行プログラムのコンテンツ識別子、記録再生器識別子を読み出し、ステップS792において、図81に示すデータ管理ファイルからコンテンツ識別子、記録再生器識別子、プログラム使用制限、記録再生器制限情報を読み出す。この場合、プログラム使用制限が「する」でコンテンツ識別子が不一致である場合、または記録再生器制限情報が「する」で記録再生器識別子が不一致である場合は、処理を終了する。【0571】次に、ステップS793、S794、S795では、データ管理ファイルの記録データにしたがって復号鍵生成処理をステップS796～S799の4種類のいずれかに設定する。【0572】「プログラム使用制限あり」の場合は、ステップS796において、コンテンツ固有鍵(ex. Kcon)と、記録再生器固有鍵(Kdev)の双方に基づいてセーブデータ復号化鍵Ksavが生成される。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵Ksavとして使用してもよい。「プログラム使用制限あり」、かつ「記録再生器制限なし」の場合は、ステップS797において、コンテンツ固有鍵(ex. Kcon)をセーブデータ復号化鍵Ksavとするか、あるいはコンテンツ固有鍵(ex. Kcon)に基づいてセーブデータ復号化鍵Ksavを生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵Ksavとして使用してもよい。【0573】「プログラム使用制限なし」、かつ「記録再生器制限あり」の場合は、ステップS798において、記録再生器固有鍵(Kdev)をセーブデータ復号化鍵Ksavとするか、あるいは記録再生器固有鍵(Kdev)に基づいてセーブデータ復号化鍵Ksavが生成される。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵Ksavとして使用してもよい。さらに、「プログラム使用制限なし」、かつ「記録再生器制限なし」の場合は、ステップS799において、システム共通鍵、例えばシステム署名鍵Ksysをセーブデータ復号化鍵Ksavとするか、あるいはシステム署名

鍵K_{s y s}に基づいてセーブデータ復号化鍵K_{s a v}を生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K_{s a v}として使用してもよい。【0576】成処理に対応する処理アルゴリズムが適用され、同一のコンテンツ固有鍵、記録再生器固有鍵に基づいて暗号化されたデータは、同一のコンテンツ固有鍵、記録再生器固有鍵に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。【0576】796～S799のいずれかにおいて生成されたセーブデータ復号化鍵を用いて復号処理が実行され、復号セーブデータが記録再生器300において再生、実行される。【0576】この図80、82において示したセーブデータ格納、再生処理フローによれば、「プログラム使用制限する」の選択がなされたセーブデータはコンテンツ固有鍵によって暗号化、復号化処理が実行されるため、同一のコンテンツ固有鍵を持つコンテンツデータを使用する場合のみ復号して利用することが可能となる。また、「記録再生器制限する」の選択がなされたセーブデータは、記録再生器識別子によって暗号化、復号化処理が実行されるため、同一の記録再生器識別子を持つ記録再生器、すなわち同一の記録再生器によってのみ復号して利用することが可能となる。従って、コンテンツ、記録再生器両者によって利用制限を設定することが可能となり、セーブデータのセキュリティをさらに高めることが可能となる。【0577】なお、図80、82においては、コンテンツ固有鍵、記録再生器固有鍵を用いたセーブデータ暗号化鍵、復号化鍵の生成構成を示したが、コンテンツ固有鍵の代わりにコンテンツ識別子、また記録再生器固有鍵の代わりに記録再生器識別子を用いて、これら識別子に基づいてセーブデータ暗号化鍵、復号化鍵の生成を実行する構成としてもよい。【0578】次に、図83～85を用いてセーブデータの暗号化鍵を生成して記録デバイスに格納する処理フローである。【0580】ステップS821において、コンテナ識別子を読み出す処理であり、前述の各処理と同様である。ステップS822は、ユーザによるプログラム使用制限の設定を行なうか否かを決定するステップである。本構成において設定されるデータ管理ファイルは、例えば図84に示す構成を持つ。【0581】図84に示す構成を持つ。【0581】

ザによるプログラム使用制限情報が含まれる。「ユーザによるプログラム使用制限情報」はプログラムを使用するユーザを制限するかしないかを設定する項目である。【0582】ステップS822において使用制限するの設定がなされると、ステップS823においてユーザパスワードの入力がなされる。この入力は、図2に示す例えればキーボード等の入力手段から入力される。【0583】入力されたパスワードは、06、制御部301の制御のもとに暗号処理部302に出力され、ステップS824における処理、すなわち入力ユーザパスワードに基づくセーブデータ暗号化鍵K_{s a v}が生成される。セーブデータ暗号化鍵K_{s a v}生成処理としては、例えればパスワード自体を暗号化鍵K_{s a v}としてもよいし、あるいは記録再生器のマスタ鍵MK_xを用いて、セーブデータ暗号化鍵K_{s a v}=DES(MK_x、パスワード)によって生成してもよい。また、パスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵を生成してもよい。【0584】ステップS828において、記録再生器300のシステム共通鍵に基づいてセーブデータ暗号化鍵が生成される。【0585】さらに、ステップS825～24、またはステップS828で生成したセーブデータ暗号化鍵K_{s a v}を用いてセーブデータの暗号化処理がなされ、ステップS826において暗号化処理のなされたセーブデータが記録デバイスに格納される。【0586】さらに4のデータ管理ファイルにステップS822で設定したユーザによるプログラム使用制限情報が、コンテンツ識別子と記録再生器識別子に対応付けられて書き込まれる。【0587】図85は、図83の処理によって格納されたセーブデータの再生処理フローを示した図である。ステップS831において、コンテンツデータからコンテンツ識別子を読み出し、ステップS832において図84に示したデータ管理ファイルからコンテンツ識別子、ユーザによるプログラム使用制限情報を読み出す。【0588】図83～85のデータに基づく判定を実行し、「ユーザによるプログラム使用制限する」が設定されている場合は、ステップS834において、パスワード入力を求め、ステップS835において、入力パスワードに基づく復号化鍵を生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、あるパスワードに基づいて暗号化されたデータは、同一のパスワードに基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムに設定される。【0589】

ログラム使用制限なしの場合は、ステップS 837において記録再生器300の内部メモリに格納されたシステム共通鍵、例えばシステム署名鍵K_{s y s}を用いてセーブデータ復号鍵K_{s a v}が生成される。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K_{s a v}として使用してもよい。【0590】ステップS 836、ステップS 837のいずれかにおいて生成された復号化鍵K_{s a v}を用いて記録デバイスに格納されたセーブデータの復号が実行され、ステップS 836において記録再生器においてセーブデータの再生、実行がなされる。【0591】図83、図85において示したセーブデータ格納、再生処理フローによれば、「ユーザによるプログラム使用制限する」の選択がなされたセーブデータはユーザ入力パスワードに基づく鍵によって暗号化、復号化処理が実行されるため、同一のパスワードを入力した場合のみ復号して利用することが可能となり、セーブデータのセキュリティを高めることが可能となる。【0592】物理、再生処理態様について説明してきたが、上述した処理を融合した処理、例えばパスワードと、記録再生器識別子、コンテンツ識別子等を任意に組み合わせて使用してセーブデータ暗号化鍵、復号化鍵を生成する態様も可能である。【0593】(17)不正機器の排除(リボケーション)構成すでに説明してきたように、本発明のデータ処理装置においては、メディア500(図3参照)、通信手段600から提供される様々なコンテンツデータを記録再生器300において、認証、暗号化処理等を実行し、記録デバイスに格納する構成によって提供コンテンツのセキュリティを高めるとともに、また、正当な利用者のみが利用可能とする構成を持つ。【0594】上述の説明から理解したところは、記録再生器300の暗号処理部302に構成される内部メモリ307に格納された様々な署名鍵、マスター鍵、チェック値生成鍵(図18参照)を用いて、認証処理、暗号化処理、復号化処理がなされる。この鍵情報を格納する内部メモリ307は、先に説明したように、基本的に外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または/かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性とした構成とされるのが望ましいが、万が一内部メモリの不正な読み取りが実行され、これらの鍵データ等が流出し、正規なライセンスのされていない記録再生器にコピーされた場合、コピーされた鍵情報に

よって不正なコンテンツ利用がなされる可能性がある。【0595】複製によるコンテンツの不正利用を防止する構成について説明する。【0596】図86に、本構成「(17)不正機器の除構成」を説明するブロック図を示す。記録再生器300は、前述の図2、3に示す記録再生器と同様であり、内部メモリを有し、先に説明した(図18)各種の鍵データ等は、記録再生器識別子を有している。なお、ここでは、第三者によって複製されている記録再生器識別子、鍵データ等は図3に示す内部メモリ307に格納されるとは限らず、図86に示す記録再生器300の鍵データ等は、暗号処理部302(図2、3参照)によってアクセス可能なメモリ部にまとめて、あるいは分散して格納されている構成であるとする。【0597】不正機器の排除コンテンツデータのヘッダ部の不正な記録再生器識別子リストを記憶した構成とした。図86に示すように、コンテンツデータには、不正な記録再生器識別子(ID dev)リストとしてのリボケーション(Revocation)リストを保有している。さらに、リボケーションリストの改竄チェック用のリストチェック値ICVrevを設けている。不正な記録再生器識別子(ID dev)リストは、コンテンツ提供者、または管理者が、例えば不正コピーの流通状態等から判明した不正な記録再生器の識別子ID devをリスト化したものである。このリボケーションリストは例えば配達鍵Kdisによって暗号化されて格納してもよい。記録再生器による復号処理については、例えば先の図22のコンテンツダウンロード処理の態様と同様である。【0598】なお、ここでは、理解を容易にするためリボケーションリストを単独のデータとして図86のコンテンツデータ中に示してあるが、例えば先に説明したところは、コンテンツデータのヘッダ部の構成要素である取扱方針(例えば図32～35参照)中にリボケーションリストを含ませてもよい。この場合は、先に説明したチェック値ICVaによってリボケーションリストを含む取扱方針データの改竄チェックがなされる。リボケーションリストが取扱方針中に含まれる場合は、チェック値A:ICVaのチェックによって代替され、記録再生器内のチェック値A生成鍵Kicvaが利用され、チェック値生成鍵Kicv-revを格納する必要はない。【0599】リボケーションリストの改竄チェック用のリストチェック値ICVrevによるリボケーションリストのチェックを実行するとともに、リストチェック値ICVrevとコンテンツデータ中の他の部分チェック値とから中間チェック値を生成して中間チェック値の検証処理を行なう構成とする。

【0600】リボケーションリストの改竄チェック用のリストチェック値ICVrevによるリボケーションリストのチェック手法は、前述の図23、図24等で説明したICVa、ICVb等のチェック値生成処理と同様の方法で実行可能である。すなわち、記録再生器暗号処理部302の内部メモリ307に保存したチェック値生成鍵Kicv-revを鍵とし、コンテンツデータ中に含まれるリボケーションリストをメッセージとして図23、図24等で説明したICV計算方法に従って計算される。計算したチェック値ICV-rev' とヘッダ(Header)内に格納されたチェック値:ICV-revを比較し、一致していた場合には、改竄が無いと判定する。【0601】リストチェック値ICVrevを含む中間チェック値は、例えば、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されている総チェック値生成鍵Kicvtを鍵とし、検証したHeader内のチェック値A、チェック値B、リストチェック値ICVrev、さらにフォーマットに応じてコンテンツチェック値を加えたメッセージ列に図7他で説明したICV計算方法を適用して生成する。【0602】これらのリエック値は、DVD、CD等のメディア500、通信手段600を介して、あるいはメモリカード等の記録デバイス400を介して記録再生器300に提供される。ここで記録再生器300は、正当な鍵データを保有する記録再生器である場合と、不正に複製された識別子IDを有する場合とがある。【0603】このような構成における排除処理の処理フローを図87および図88に示す。図87は、DVD、CD等のメディア500、あるいは通信手段600からコンテンツが提供される場合の不正記録再生器排除(リボケーション)処理フローであり、図88は、メモリカード等の記録デバイス400からコンテンツが提供される場合の不正記録再生器排除(リボケーション)処理フローである。【0604】まず、図87に示す処理は、ステップ901は、メディアを装着して、コンテンツの提供、すなわち再生処理あるいはダウンロードの要求を行なうステップである。この図87に示す処理は、例えば記録再生器にDVD等のメディアを装着してダウンロード処理等を実行する前のステップとして実行される。ダウンロード処理については、先に図22を用いて説明している通りであり、図22の処理フローの実行の前ステップとして、あるいは図22の処理フロー中に挿入される処理としてこの図87の処理が実行される。【0605】手段を介してコンテンツ提供を受ける場合は、ステップS911においてコンテンツ配信サービス側との通信セッションを確立し、その後、ステップS902へ進む。

【0606】ステップS902では、コンテンツデータのヘッダ部からリボケーションリスト(図86参照)を取得する。このリスト取得処理は、コンテンツがメディア内にある場合は、図3に示す制御部301が読み出し部304を介してメディアから読み出し、コンテンツが通信手段からである場合は、図3に示す制御部301が通信部305を介してコンテンツ配信側から受信する。【0607】次に01は、暗号処理部302にメディア500または通信手段600から取得したリボケーションリストを暗号処理部302に渡し、チェック値生成処理を実行させる。記録再生器300は、内部にリボケーションチェック値生成鍵Kicv-revを有し、受領したリボケーションリストをメッセージとしてリボケーションチェック値生成鍵Kicv-revを適用して、例えば図23、図24等で説明したICV計算方法に従ってチェック値ICV-rev'を計算し、計算結果とコンテンツデータのヘッダ(Header)内に格納されたチェック値:ICV-revを比較し、一致していた場合には改竄が無い(ステップS904でYes)と判定する。一致しない場合は、改竄されていると判定され、ステップS909に進み処理エラーとして処理を終了する。【0608】次に、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308に総チェック値ICVt'の計算をさせる。総チェック値ICVt'は、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているシステム署名鍵Ksysを鍵とし、中間チェック値DESで暗号化して生成する。なお、各部分チェック値、例えばICVa、ICVb等の検証処理は、この図87に示す処理フロー中では省略してあるが、先に説明した図39～図45の処理フローと同様の各データフォーマットに応じた部分チェック値の検証が行なわれる。【0609】次に、ステップS907のた総チェック値ICVt' とヘッダ(Header)内のICVtを比較し、一致していた場合(ステップS906でYes)には、ステップS907へ進む。一致しない場合は、改竄されていると判定され、ステップS909に進み処理エラーとして処理を終了する。【0610】先に説明したtは、ICVa、ICVb、さらに、データフォーマットに応じて各コンテンツブロックのチェック値等、コンテンツデータに含まれる部分チェック値全体をチェックするものであるが、ここでは、これらの部分チェック値060にさらに、リボケーションリストの改竄チェック用のリストチェック値ICVrevを部分チェック値として加えて、これら全ての改竄を検証する。上述の処理によって生成された総チェック値がヘッダ(Header)内に格納されたチェック値:ICVtと一致した場合には、IC

V a、 I C V b、各コンテンツブロックのチェック値、およびリストチェック値 I C V r e v 全ての改竄はないと判断される。【0611】さらにステップ S 907 では、改すなわち不正な記録再生器識別子 I D d e v をリスト化したリボケーションリストと、自己の記録再生器 300 に格納された記録再生器識別子 (I D d e v) との比較がなされる。【0612】コンテンツデータから読み出された記録再生器識別子 I D d e v のリストに自己の記録再生器の識別子 I D d e v が含まれている場合は、その記録再生器 300 は、不正に複製された鍵データを有していると判定され、ステップ S 909 に進み、以後の手続きは中止される。例えば図 22 のコンテンツダウンロード処理の手続きの実行を不可能とする。【0613】ステップ S 905 利用を排除することが可能となる。【0617】(18) セキ法先に説明したように、記録再生器暗号処理部 302 の内部メモリ 307、あるいは記録デバイス 400 の内部メモリ 405 は、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従って、記録再生器暗号処理部 302、記録デバイス暗号処理部 401 は、例えば外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する耐タンパメモリとして構成される。【0618】しかしながら、上述の説明で現に、例えば記録再生器暗号処理部 302 の内部メモリ 307 には記録再生器署名鍵 K d e v 等の記録再生器毎に異なるデータを書き込むことが必要となる。また、チップ内の不揮発性の記憶領域、例えばフラッシュメモリ、F e R A M 等にチップ毎の個別情報、例えば識別情報 (I D) や暗号鍵情報を書き込んだ後、例えば製品出荷後におけるデータの再書き込み、読み出しを困難とする必要となる。【0619】従来の書き込みデータの読み込み処理を困難とするための手法には、例えばデータ書き込みのコマンドプロトコルを秘密にする。あるいは、チップ上のデータ書き込みコマンドを受け付ける信号線と、製品化した後に利用される通信用の信号線を分離して構成し、基板上のチップに直接信号を送らない限りデータ書き込みコマンドが有効とならないようにする等の手法がある。【0620】しかしながら、このような従来手法をしても、記憶素子の専門知識を有するものにとっては、回路を駆動させる設備と技術があれば、チップのデータ書き込み領域に対する信号出力が可能であり、また、たとえデータ書き込みのコマンドプロトコルが秘密であつたとしても、プロトコルの解析可能性は常に存在する。【0621】

いては、コンテンツ提供者、または管理者が提供するコンテンツに併せて不正な記録再生器を識別するデータ、改すなわち不正な記録再生器識別子 I D d e v をリスト化したリボケーションリストをコンテンツデータのヘッダ部の構成データとして含ませて記録再生器利用者に提供し、記録再生器利用者は、記録再生器によるコンテンツの利用に先立って、自己の記録再生器のメモリに格納された記録再生器識別子 I D d e v と、リストの識別子との照合を実行して一致するデータが存在した場合には、以後の処理を実行させない構成としたので鍵データを複製してメモリに格納した不正な記録再生器によるコンテンツ利用を排除することが可能となる。【0617】(18) セキ法先に説明したように、記録再生器暗号処理部 302 の内部メモリ 307、あるいは記録デバイス 400 の内部メモリ 405 は、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従って、記録再生器暗号処理部 302、記録デバイス暗号処理部 401 は、例えば外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する耐タンパメモリとして構成される。【0618】しかしながら、上述の説明で現に、例えば記録再生器暗号処理部 302 の内部メモリ 307 には記録再生器署名鍵 K d e v 等の記録再生器毎に異なるデータを書き込むことが必要となる。また、チップ内の不揮発性の記憶領域、例えばフラッシュメモリ、F e R A M 等にチップ毎の個別情報、例えば識別情報 (I D) や暗号鍵情報を書き込んだ後、例えば製品出荷後におけるデータの再書き込み、読み出しを困難とする必要となる。【0619】従来の書き込みデータの読み込み処理を困難とするための手法には、例えばデータ書き込みのコマンドプロトコルを秘密にする。あるいは、チップ上のデータ書き込みコマンドを受け付ける信号線と、製品化した後に利用される通信用の信号線を分離して構成し、基板上のチップに直接信号を送らない限りデータ書き込みコマンドが有効とならないようにする等の手法がある。【0620】しかしながら、このような従来手法をしても、記憶素子の専門知識を有するものにとっては、回路を駆動させる設備と技術があれば、チップのデータ書き込み領域に対する信号出力が可能であり、また、たとえデータ書き込みのコマンドプロトコルが秘密であつたとしても、プロトコルの解析可能性は常に存在する。【0621】

持した暗号処理データの格納素子を流通させることは、暗号処理システム全体を脅かす結果となる。また、データの読み出しを防止するために、データ読み出しコマンド自体を実装しない構成とすることも可能であるが、その場合、正規のデータ書き込みを実行した場合であっても、メモリに対するデータ書き込みが実際に行われたか否かを確認したり、書き込まれたデータが正確に書き込まれているか否かを判定することが不可能となり、不良なデータ書き込みの行われたチップが供給される可能性が発生する。【0622】これらの従来技術に鑑み、ここでは例えばフラッシュメモリ、F e R A M等の不揮発性メモリに正確なデータ書き込みを可能とするとともに、データの読み出しを困難にするセキュアチップ構成およびセキュアチップ製造方法を提供する。【0623】図89に、データ処理部302または記録デバイス400の暗号処理部401に適用可能なセキュリティチップ構成を示す。図89(A)はチップの製造過程、すなわちデータの書き込み過程におけるセキュリティチップ構成を示し、図89(B)は、データを書き込んだセキュリティチップを搭載した製品の構成例、例えば記録再生器300、記録デバイス400の例を示す。【0624】製造過程にあるセキュリティチップ構成を示す。図89(A)は、モード指定用信号線8003、および各種コマンド信号線8004が接続され、処理部8001は、モード指定用信号線8003で設定されたモード、例えばデータ書き込みモードまたはデータ読み出しモードに応じて不揮発性メモリである記憶部8002へのデータ書き込み処理、または記憶部8002からのデータ読み出し処理を実行する。【0625】一方、図89(B)は、データを書き込んだセキュリティチップを搭載した製品においては、セキュリティチップと外部接続インターフェース、周辺機器、他の素子等とが汎用信号線で接続されるが、モード信号線8003は、非接続状態とされる。具体的な処理は、例えばモード信号線8003をグランド接続する、Vccに釣り上げる、信号線をカットする、あるいは絶縁体樹脂で封印する等である。このような処理により、製品出荷後は、セキュリティチップのモード信号線に対するアクセスが困難になり、外部からチップのデータを読み出したり書き込みを行なったりすることの困難性を高めることができる。【0626】一方、データの記憶部8002に対する書き込み処理、および記憶部8002に書き込まれたデータの読み出し処理を困難にする構成を持ち、たとえ第三者がモード信号線8003のアクセスに成功した場合であっても不正なデータ書き込み、読み出しを防止可能である。図90に本構成を有するセキュリティチップにおけるデータ書き込みまたは読み出し処理フローを示す。

【0627】ステップS951は、モード信号線8003をデータ書き込みモードまたはデータ読み出しモードに設定するステップである。【0628】ステップS952は、データを取り出すステップである。本構成のセキュリティチップには、例えばワイヤ(Wire)、マスクROM構成により、予めパスワード、暗号技術における認証処理用の鍵情報等、認証処理に必要な情報が格納される。ステップS952は、この認証情報を読み出して認証処理を実行する。例えば正規なデータ書き込み治具、データ読み出し装置を汎用信号線に接続して認証処理を実行した場合には、認証OK(ステップS953においてYes)の結果が得られるが、不正なデータ書き込み治具、データ読み出し装置を汎用信号線に接続して認証処理を実行した場合には、認証に失敗(ステップS953においてNo)し、その時点で処理が中止される。認証処理は、例えば先に説明した図13の相互認証処理手続きに従って実行可能である。図89に示す処理部8001は、これらの認証処理を実行可能な構成を有する。これは、例えば先に説明した図29に示す記録デバイス400の暗号処理部401の制御部403に組み込まれたコマンドレジスタと同様の構成により実現可能である。例えば図89のチップの処理部は、図29に示す記録デバイス400の暗号処理部401の制御部403に組み込まれたコマンドレジスタと同様の構成を持ち、各種コマンド信号線8004に接続された機器から所定のコマンドNoが入力されると、対応する処理を実行し、認証処理シーケンスを実行することができる。【0629】処理部8001のなされた場合にのみ、データの書き込みコマンド、またはデータの読み出しコマンドを受け付けてデータの書き込み処理(ステップS955)、またはデータの読み出し処理(ステップS956)を実行する。【0630】このようにおいては、データの書き込み時、読み出し時に認証処理を実行する構成としたので、正当な権利を持たない第三者によるセキュリティチップの記憶部からデータの読み出し、または記憶部へのデータ書き込みを防止することができる。【0631】次に、さらに、セキュリティの高い素子構成とした実施例を図91に示す。この例では、セキュリティチップの記憶部8200が2つの領域に分離され、一方はデータの読み書きが可能な読み出し書き込み併用領域(RW: Read Write領域)8201であり、他方はデータの書き込みのみが可能な書き込み専用領域(WO: Write Only領域)8202である。【0632】O: Write Only領域)8202には、暗号鍵データ、識別子データ等のセキュリティ要請の高いデータを書き込み、一方セキュリティ度のさほど高くない、例

えばチェック用のデータ等を読み出し書き込み併用領域(RW: Read Write領域)8201に書き込む。【062】領域(RW: Read Write領域)8201からのデータ読み出し処理は、前述の図90で説明した認証処理を伴うデータ読み出し処理を実行する。しかし、データ書き込み処理は、図92のフローに従って実行する。【063】線8003を書き込みモードに設定するステップであり、ステップ962では、先の図90で説明したと同様の認証処理を実行する。認証処理で認証がなされると、ステップS963に進み、コマンド信号線8004を介して、書き込み専用(WO)領域8202にセキュリティの高い鍵データ等の情報の書き込み、読み出し書き込み併用領域(RW: Read Write領域)8201にセキュリティ度のさほど高くない、例えばチェック用データ書き込むコマンドを処理部8001に対して出力する。【0635】ステップS964ではコマンドを受領した処理部8001が、コマンドに応じたデータ書き込み処理をそれぞれ書き込み専用(WO)領域8202、読み出し書き込み併用領域(RW: Read Write領域)8201に対して実行する。【0636】また、書き込み専用に書き込まれたデータの検証処理フローを図93に示す。【0637】図93のステップS971は、処理部8001において、書き込み専用(WO)領域8202に書き込まれたデータに基づく暗号処理を実行させる。これらの実行構成は、先の認証処理実行構成と同様、コマンドレジスタに格納された暗号処理シーケンスを順次実行する構成によって実現される。また、処理部8001において実行される暗号処理アルゴリズムは特に限定されるものではなく、例えば先に説明したDESアルゴリズムを実行する構成とすることができます。【0638】次に、チップに接続された検証装置が処理部8001から暗号処理結果を受信する。次に、ステップS973において、先に記憶部に書き込み処理を行なった正規な書き込みデータに対して処理部8001において実行されたアルゴリズムと同様の暗号化処理を適用して得た結果と、処理部8001からの暗号化結果とを比較する。【0639】セーブデータ領域8202に書き込まれたデータは正しいことが検証される。【0640】この構成では、認証処理が破られて読み出しへコマンドが万が一実行可能となつても、データの読み出し可能領域は、読み出し書き込み併用領域(RW: Read Write領域)8201に限定され、書き込み専用(WO)領域8202に書き込まれたデータの読み

出しは、不可能であり、さらにセキュリティの高い構成となる。また、全く読み出しを不可能としたチップと異なり、読み出し書き込み併用領域(RW: Read Write領域)8201が構成されているのでメモリアクセスの正否チェックが可能である。【0641】以上、特定の実用について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。また、上記した実施例ではコンテンツの記録、再生を可能な記録再生器を例にして説明してきたが、データ記録のみ、データ再生のみ可能な装置においても本発明の構成は適用可能なものであり、本発明はパソコン用コンピュータ、ゲーム機器、その他の各種データ処理装置一般において実施可能なものである。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参考すべきである。【0642】【発明の効果】上述した生器およびセーブデータ処理方法は、プログラムのみに固有な暗号鍵、例えばコンテンツ鍵を用いて、あるいはコンテンツ鍵に基づいて生成したセーブデータ暗号鍵を用いてセーブデータを暗号化して記録デバイスに格納可能な構成とし、さらに、記録再生器固有の鍵、例えば記録再生器署名鍵を用いてセーブデータ暗号鍵を生成してセーブデータを暗号化して記録デバイスに格納する構成としたので、プログラムの同一性、あるいは記録再生器の同一性等が確保された場合にのみセーブデータを利用することが可能となり、セーブデータの不正な第三者による利用、改竄等を防止可能となる。【0643】さらに、本発明のセーブデータ処理方法によれば、ユーザの固有情報、例えば入力パスワードに基づいてセーブデータの暗号鍵を生成してユーザ固有のセーブデータ暗号鍵によるセーブデータ格納を可能とした。また、このような各種の利用制限、すなわちプログラムの同一性、記録再生器の同一性、ユーザの同一性を適宜組み合わせてセーブデータの利用制限を付して記録デバイスに格納することができ、セキュリティの高いセーブデータの格納、再生処理が可能となる。

【図面の簡単な説明】【図1】従来のデータ処理システムの構成を示す。【図2】本発明の適用されるデータ処理装置の構成を示す図である。【図3】本発明の適用されるデータ処理装置の構成を示す図である。【図4】メディア上、通信路上におけるコンテンツデータのデータフォーマットを示す図である。

【図5】コンテンツデータ中のヘッダに含まれる取扱方
 針を示す図である。【図6】コンテンツデータ中のヘッダに含おけるコマンド実行方法について説明する図である。【図32】ニ
 ク情報を示す図である。【図7】DESを用いた電子署名生成ト・タイプ0の構成を説明する図である。【図33】コンテンツラ
 する。【図8】トリプルDESを用いた電子署名生成方法を示す図である。【図34】ト・タイプ1の構成を説明する図である。【図35】コンテンツラ
 す図である。【図9】トリプルDESの構成を説明する図である。【図10】ト・タイプ2の構成を説明する図である。【図11】コンテンツラ
 方法を示す図である。【図12】電子署名生成における処理フローを示す図である。【図13】チェック値ICViの生成処理方法を説明する図であ
 ある。【図14】対称鍵暗号技術を用いた相互認証処理の処理フローを示す図である。【図15】フォーマット・タイプ1におけるコンテンツ
 シーケンスを説明する図である。【図16】公開鍵証明書を用いた相互認証処理の処理フローを示す図である。【図17】楕円曲線暗号を用いた
 フォーマット・タイプ2、3における総チェック値の生成処理方法を説明する図である。【図18】楕円曲線暗号を用いた復号化処理の処理フローを示す図である。【図19】記録再生器上のデータ保持状況を示す図である。【図20】記録再生器と記録デバイスとの相互認証処理の処理フローを示す図である。【図21】記録再生器のマスタ鍵と記録再生器との相互認証処理の処理フローを示す図である。【図22】フォーマット・タイプ0、1におけるデータ保持状況を示す図である。【図23】チェック値A:ICVaの再生処理の処理フローを示す図である。【図24】チェック値B:ICVbの生成方法を説明する図である。【図25】総チェック値、記録再生器固有チェック値の生成処理の処理フローを示す図である。【図26】記録デバイスに保存するチェック値の生成、検証方法を説明する図(その1)
 のフォーマット(利用制限情報=0)を示す図である。【図27】コンテンツ生成者と、コンテンツ検証者におけるデータ保持状況を示す図である。【図28】コンテンツ生成者と、コンテンツ検証者における相互認証処理の処理フローを示す図である。【図29】記録デバイスにおけるコマンド実行方法を説明する図である。【図30】記録デバイスにおけるコンテンツデータの構成を示す図である。

【図31】記録デバイスにおけるコンテンツ再生処理に
 する。【図32】ト・タイプ1の構成を説明する図である。【図33】ト・タイプ2の構成を説明する図である。【図34】コンテンツラ
 す図である。【図35】ト・タイプ3の構成を説明する図である。【図36】フォーマット・タイプ1におけるコンテンツ
 シーケンスを説明する図である。【図37】フォーマット・タイプ1におけるコンテンツの生成処理方法を説明する図である。【図38】フォーマット・タイプ2、3における総チェック値の生成処理方法を説明する図である。【図39】楕円曲線暗号を用いた復号化処理の処理フローを示す図である。【図40】記録再生器上のデータ保持状況を示す図である。【図41】記録再生器と記録デバイスとの相互認証処理の処理フローを示す図である。【図42】記録再生器のマスタ鍵と記録再生器との相互認証処理の処理フローを示す図である。【図43】フォーマット・タイプ0、1におけるデータ保持状況を示す図である。【図44】チェック値A:ICVaの再生処理の処理フローを示す図である。【図45】チェック値B:ICVbの生成方法を説明する図である。【図46】総チェック値、記録再生器固有チェック値の生成処理の処理フローを示す図である。【図47】記録デバイスに保存するチェック値の生成、検証方法を説明する図(その1)
 のフォーマット(利用制限情報=0)を示す図である。【図48】コンテンツ生成者と、コンテンツ検証者におけるデータ保持状況を示す図である。【図49】コンテンツ生成者と、コンテンツ検証者における相互認証処理の処理フローを示す図である。【図50】記録デバイスにおけるコマンド実行方法を説明する図である。【図51】記録デバイスにおけるコンテンツデータの構成を示す図である。

【図5.2】マスタ鍵の使い分けにより、利用制限を実行する構成について説明する図である。【図5.3】マスタ鍵方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例3）である。【図5.4】マスタ鍵

方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例4）である。【図55】マスタ鍵方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図（例5）である。【図56】トリプルDESアルゴリズムを用いて格納する処理フローを示す図である。【図57】優先順位に基づくコンテンツ再生

(例 1) を示す図である。【図 5 8】優先順位に基づく
(例 2) を示す図である。【図 5 9】優先順位に基づく
(例 3) を示す図である。【図 6 0】コンテンツ再生処
号(伸長)処理を実行する構成について説明する図であ

る。【図6.1】コンテンツの構成例（例1）を示す図である。【図6.2】コンテンツの構成例1における再生処理一を示す図である。【図6.3】コンテンツの構成例（例2）を示す図である。【図6.4】コンテンツの構成例2における再生処理一を示す図である。

る。【図 6-4】コンテンツの構成例 2における再生処理一を示す図である。【図 6-5】コンテンツの構成例（例る。【図 6-6】コンテンツの構成例 3における再生処理一を示す図である。【図 6-7】コンテンツの構成例（例

る。【図6.8】コンテンツの構成例4における再生処理一を示す図である。【図6.9】セーブデータの生成、格する図である。【図7.0】セーブデータの格納処理例(修理フロー)を示す図である。【図7.1】セーブデータの格

されるデータ管理ファイル構成（例1）を示す図である。【図7-2】セーブデータの再生処理例（例1）に関するフローを示す図である。【図7-3】セーブデータの格

【図74】セーブデータの再生処理例(例2)に関する処理フローを示す図である。【図75】セーブデータの格納処理例(例2)に関する処理フローを示す図である。【図76】セーブデータの格納、再生されるデータ管理ファイル構成(例2)を示す図である。

る。【図 7.7】セーブデータの再生処理例(例 3)に関する処理フローを示す図である。【図 7.8】セーブデータの格納処理例(例 3)に関する処理フローを示す図である。【図 7.9】セーブデータの再生処理例(例 3)に関する処理フローを示す図である。【図 8.0】セーブデータの格納処理例(例 3)に関する処理フローを示す図である。【図 8.1】セーブデータの格納、再生されるデータ管理ファイル構成(例 3)を示す図である。

る。【図8.5】セーブデータの再生処理例(例6)に関する処理フローを示す図である。【図8.6】コンテンツ不正利用者排除構成を説明する図である。【図8.7】コンテンツ不正利用者排除の処理フロー(例1)を示す図である。【図8.8】コンテンツ

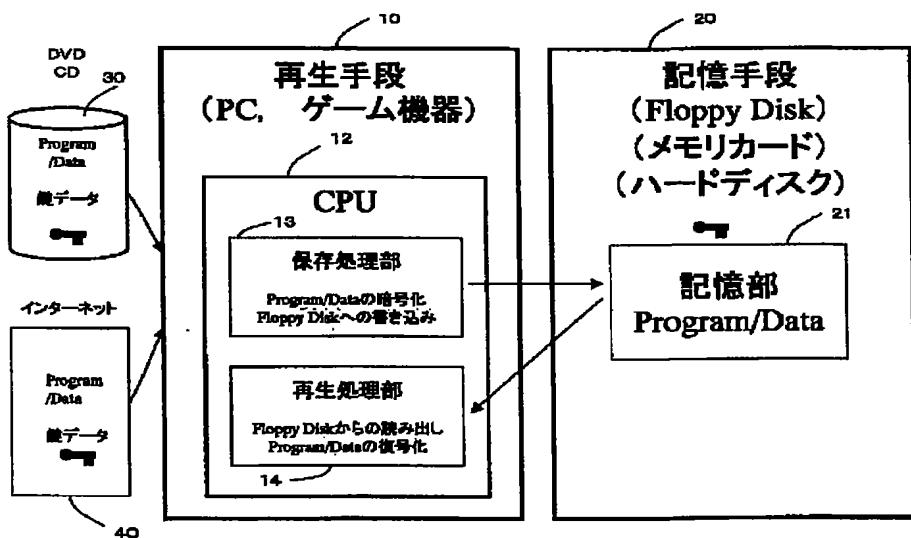
ン）の処理フロー（例1）を示す図である。【図8-8】（ノンノンセンス）の処理フロー（例2）を示す図である。【図8-9】セキュリティの図である。【図9-0】セキュリティチップの製造方法における処理フローを示す図である。【図9-1】セキュリティチップの構成（例）

る図である。【図92】セキュリティチップ(例2)におけるデータ書き込み処理における処理フローを示す図である。【図93】セキュリティチップ(例2)におけるデータチェック処理における処理フローを示す図である。

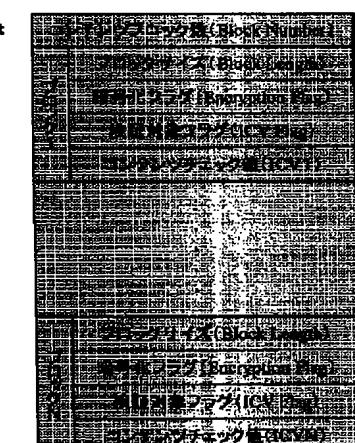
例題(例2)に関する処

1 1 1 P I O 1 1 2 S I O 3 0 0 記録再生器 3 0 1 制 2 1 0 4, 2 1 0 5, 2 1 0 6 記録デバイス 2 9 0 1 コマンド

[図1]

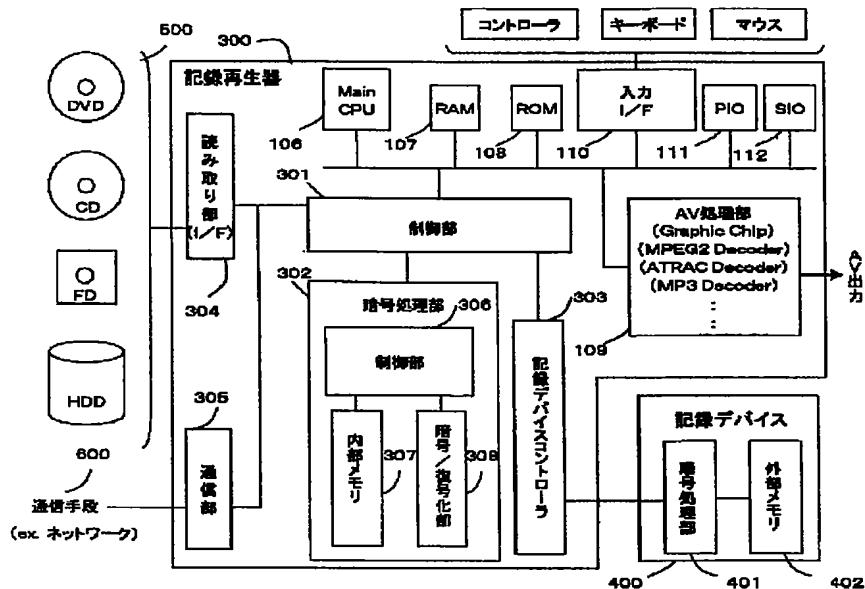


【図6】

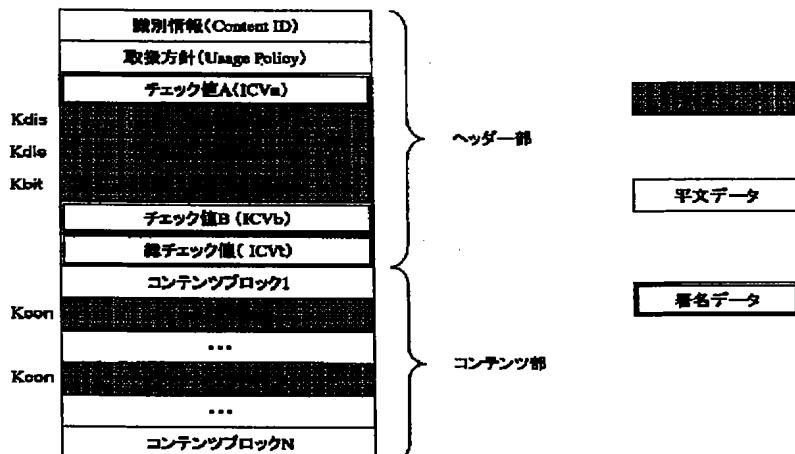


ブロック情報

【図2】



【図4】



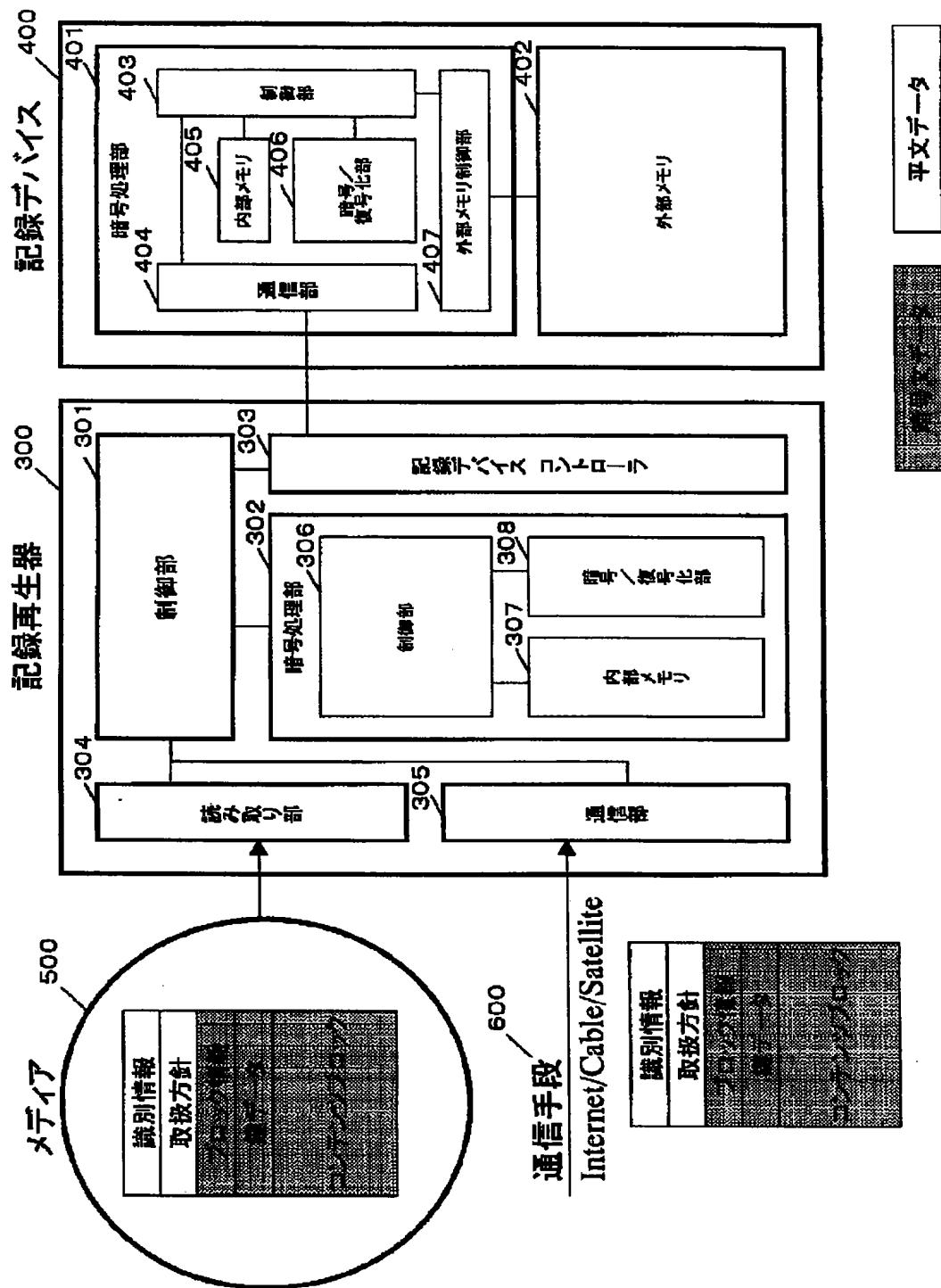
メディア上及び通信路上のデータフォーマット

【図5】

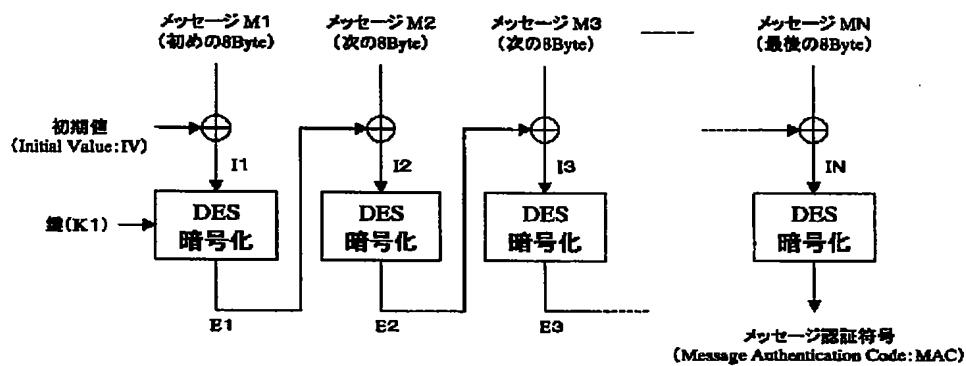
ヘッダーサイズ (Header Length)
コンテンツサイズ (Content Length)
フォーマットバージョン (Format Version)
フォーマットタイプ (Format Type)
コンテンツタイプ (Content Type)
起動優先順位情報 (Operation Priority)
利用制限情報 (Localization Field)
複数制限情報 (Copy Permission)
移動制限情報 (Move Permission)
暗号アルゴリズム (Encryption Algorithm)
暗号化モード (Encryption Mode)
検証方法 (Integrity Check Method)

取扱方針

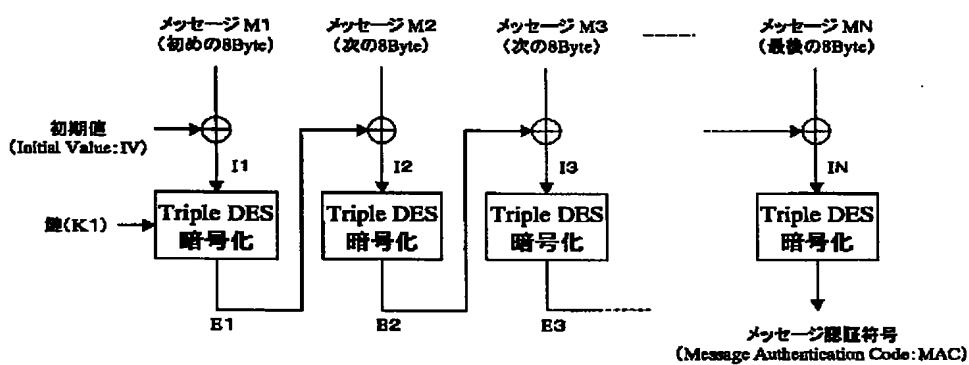
【図3】



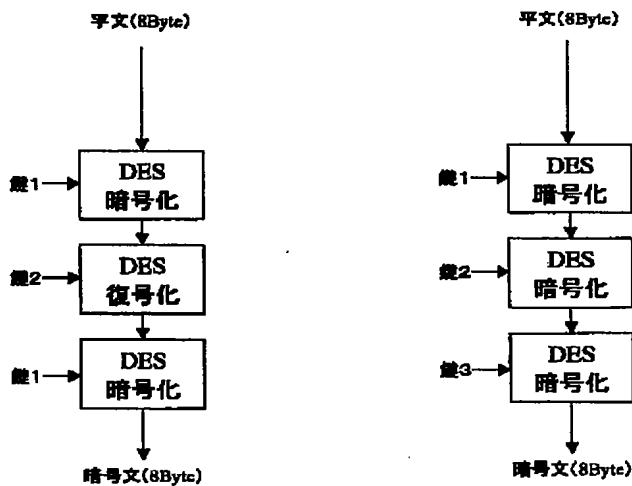
【図 7】



【図 8】

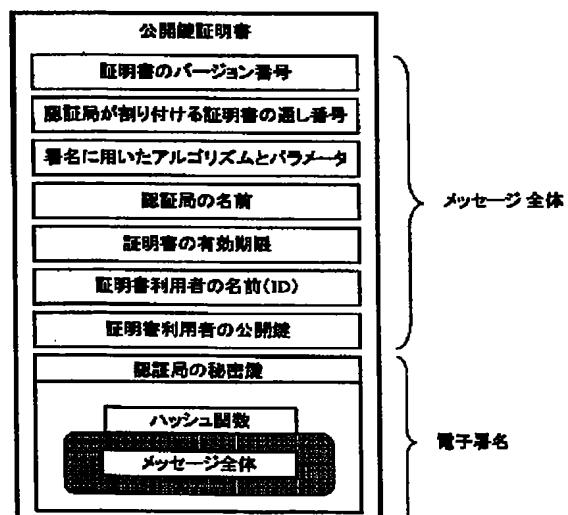


【図 9】



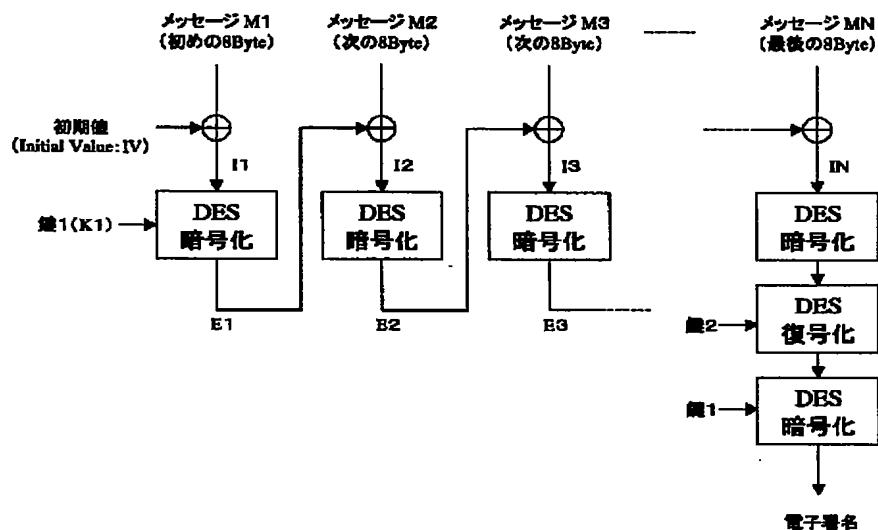
(a)

(b)



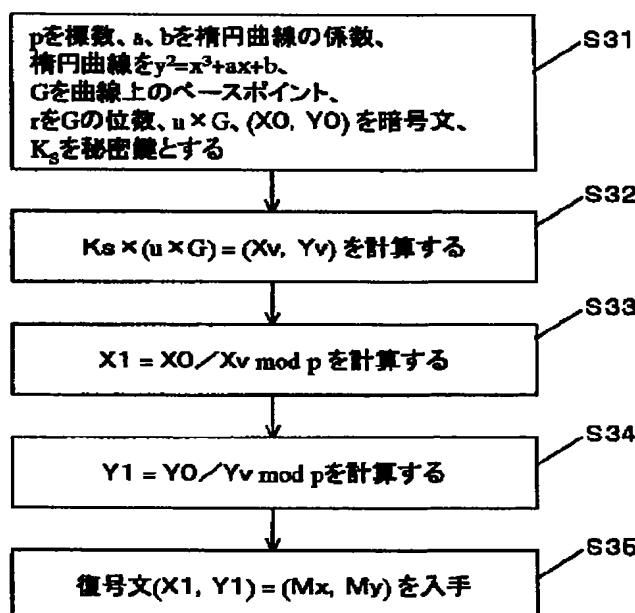
公開鍵証明書

【図10】



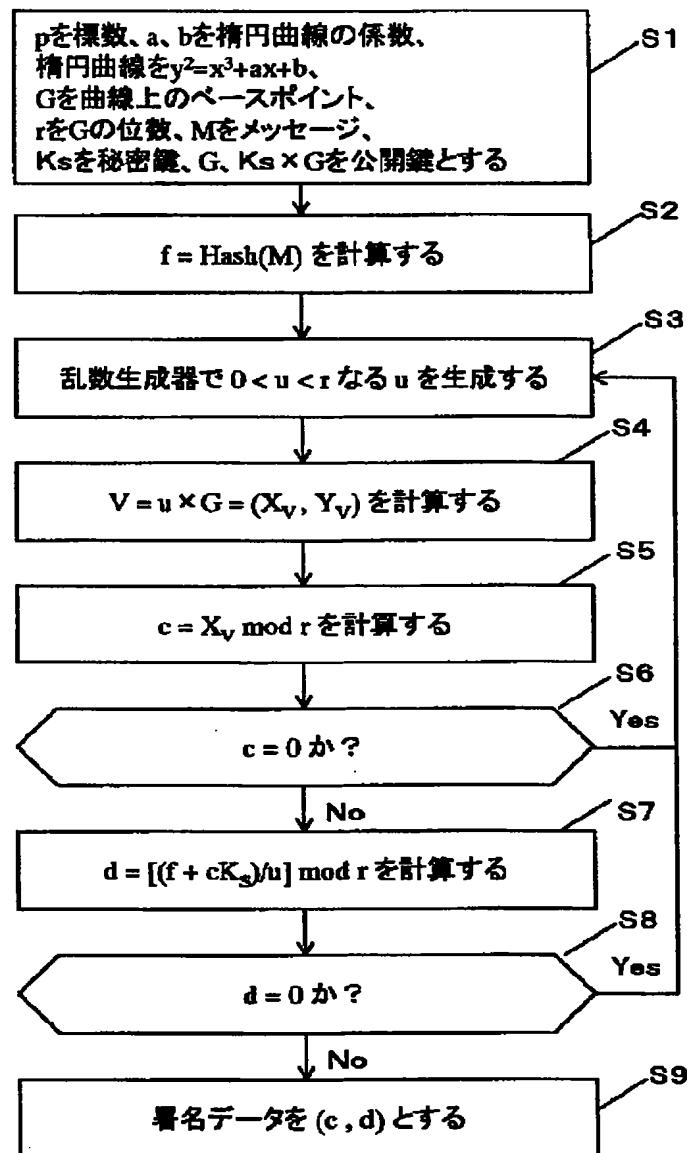
【図17】

復号化



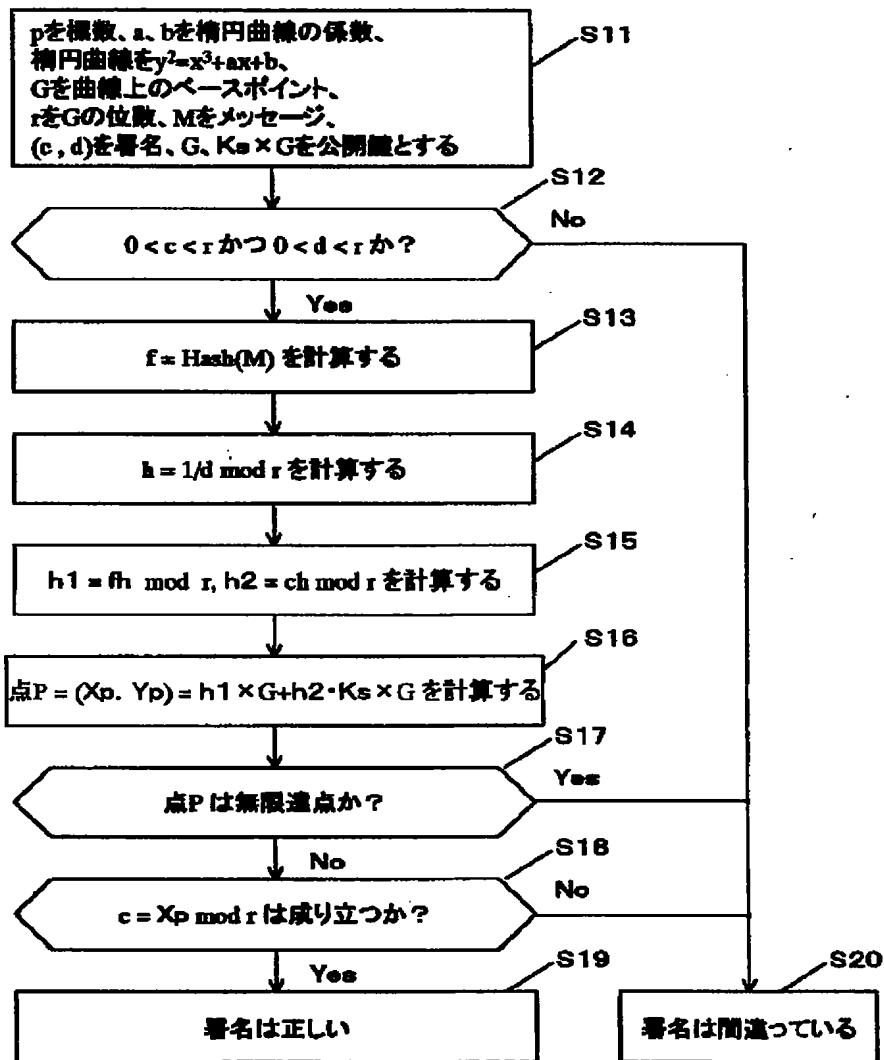
椭円曲線暗号を用いた復号化(Menezes-Vanstone)

【図11】

署名生成署名生成(IEEE P1363/D3)

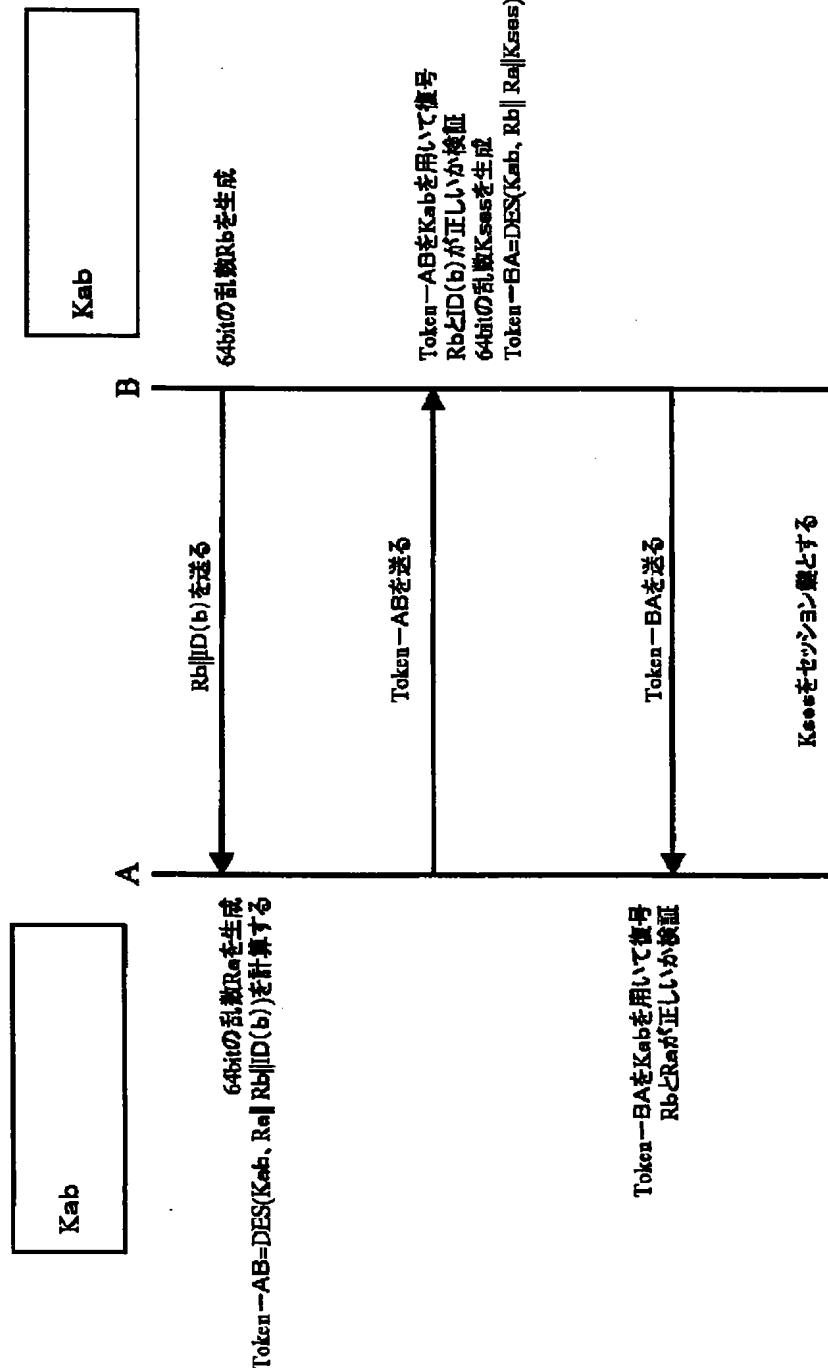
【図12】

署名検証



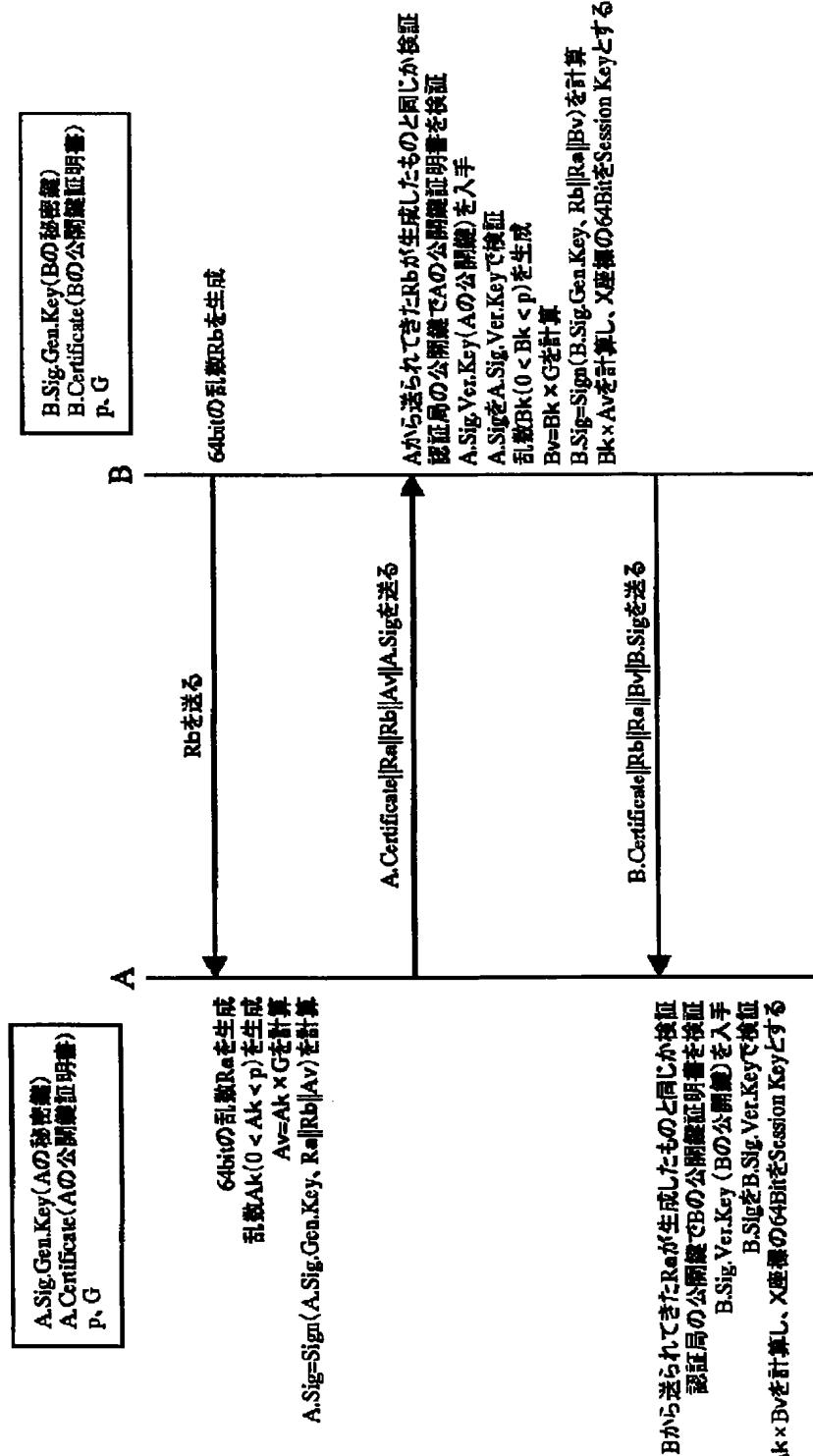
署名検証(IEEE P1363/D3)

【図13】



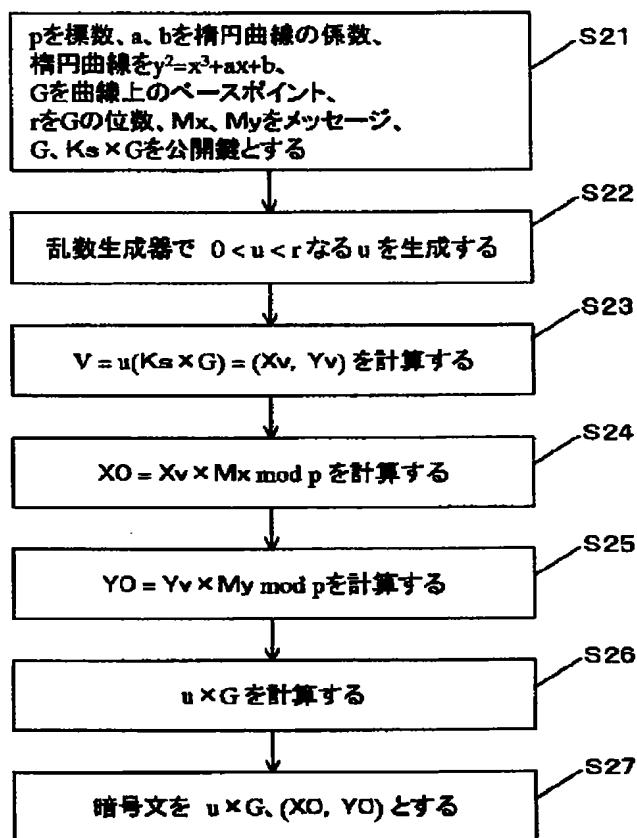
ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

【図15】

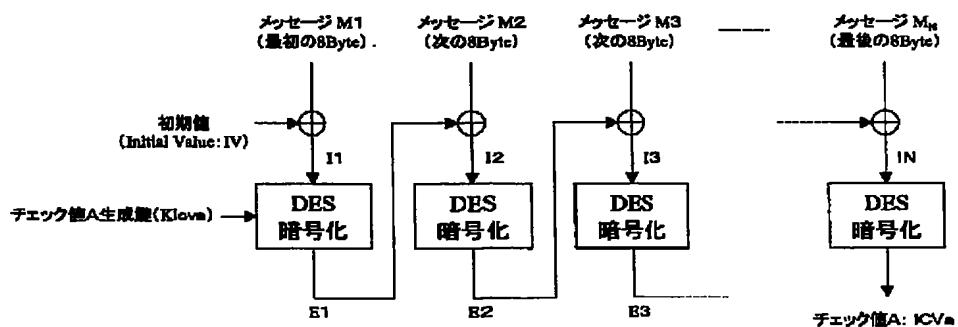


ISO/IEC 9798-3 非対称鍵暗号技術を用いた相互認証および鍵共有方式

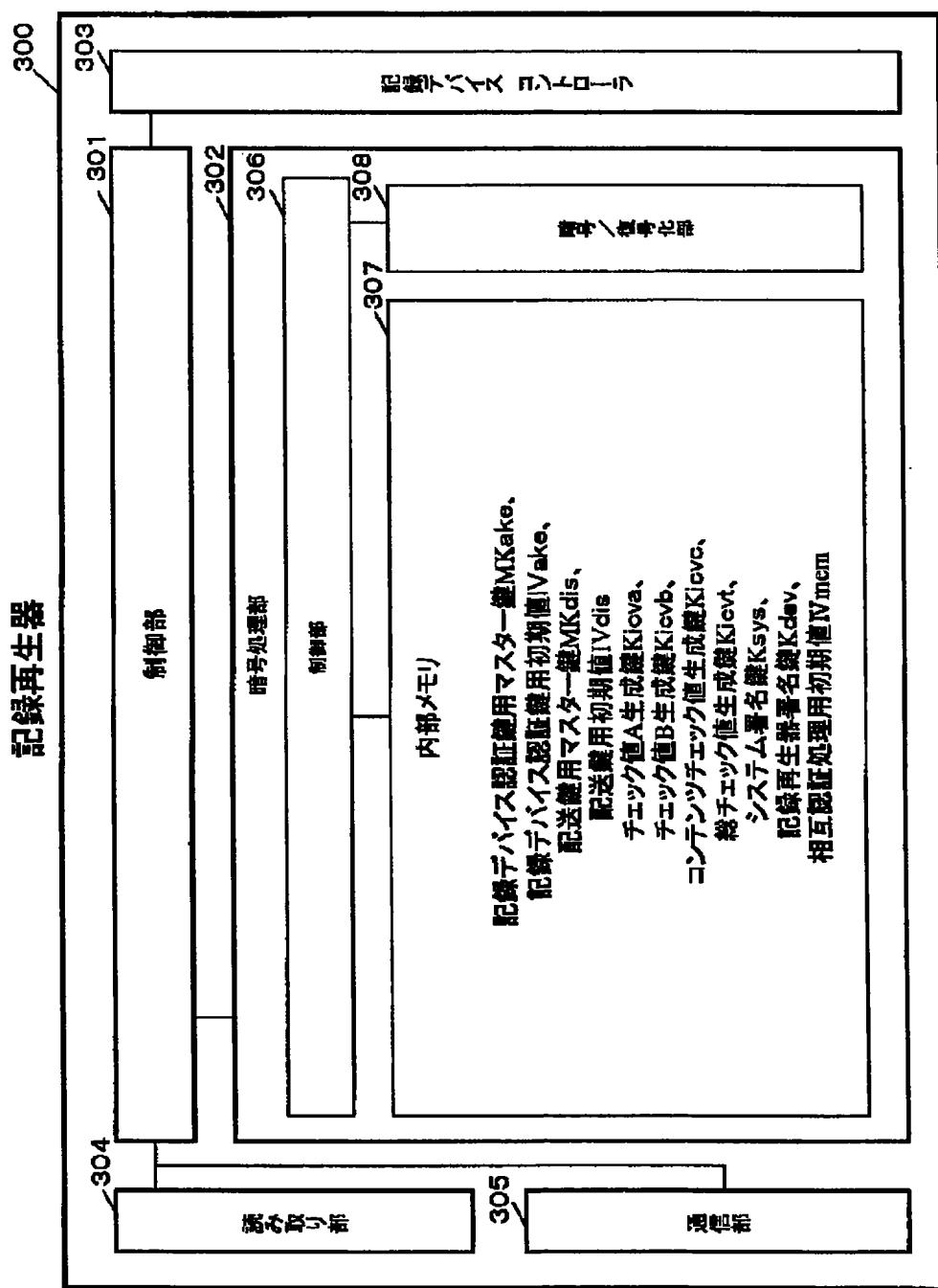
【図16】

暗号化椭円曲線暗号を用いた暗号化(Menezes-Vanstone)

【図23】

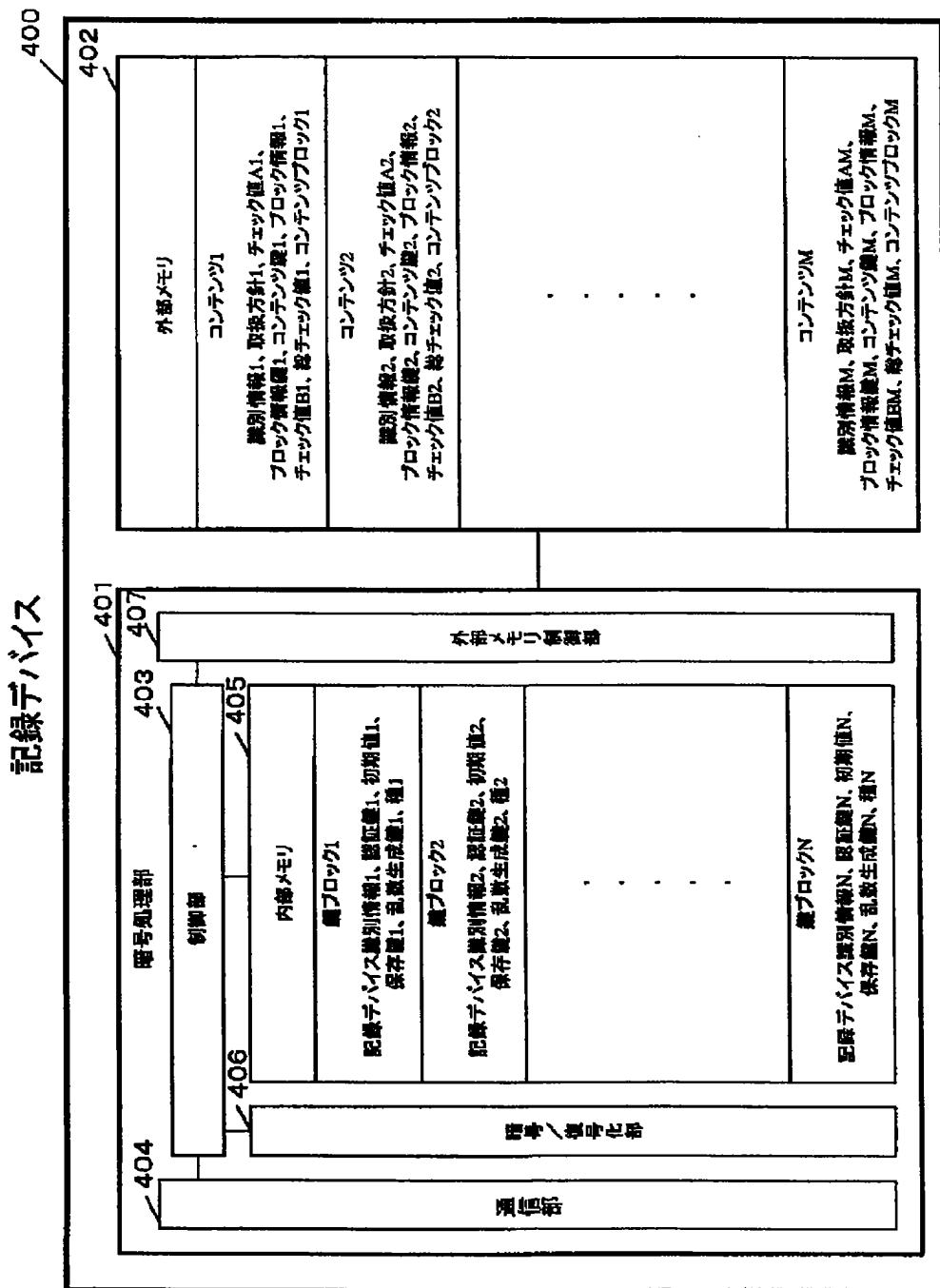
メッセージ $M_1 \sim M_n$: 識別情報、取扱方針
 \oplus : 他の論理和処理(8バイト単位)

【図18】



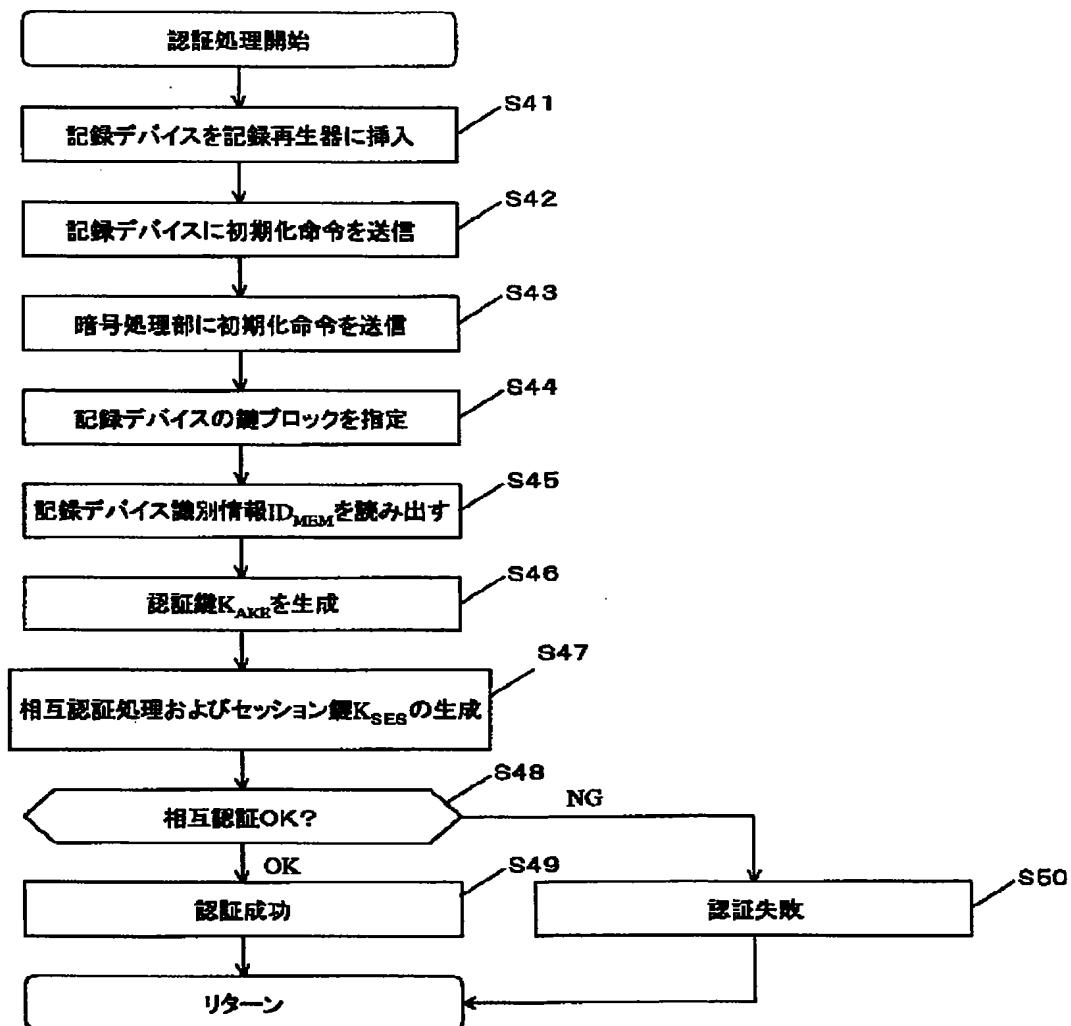
記録再生器上のデータ保持状況

【図19】



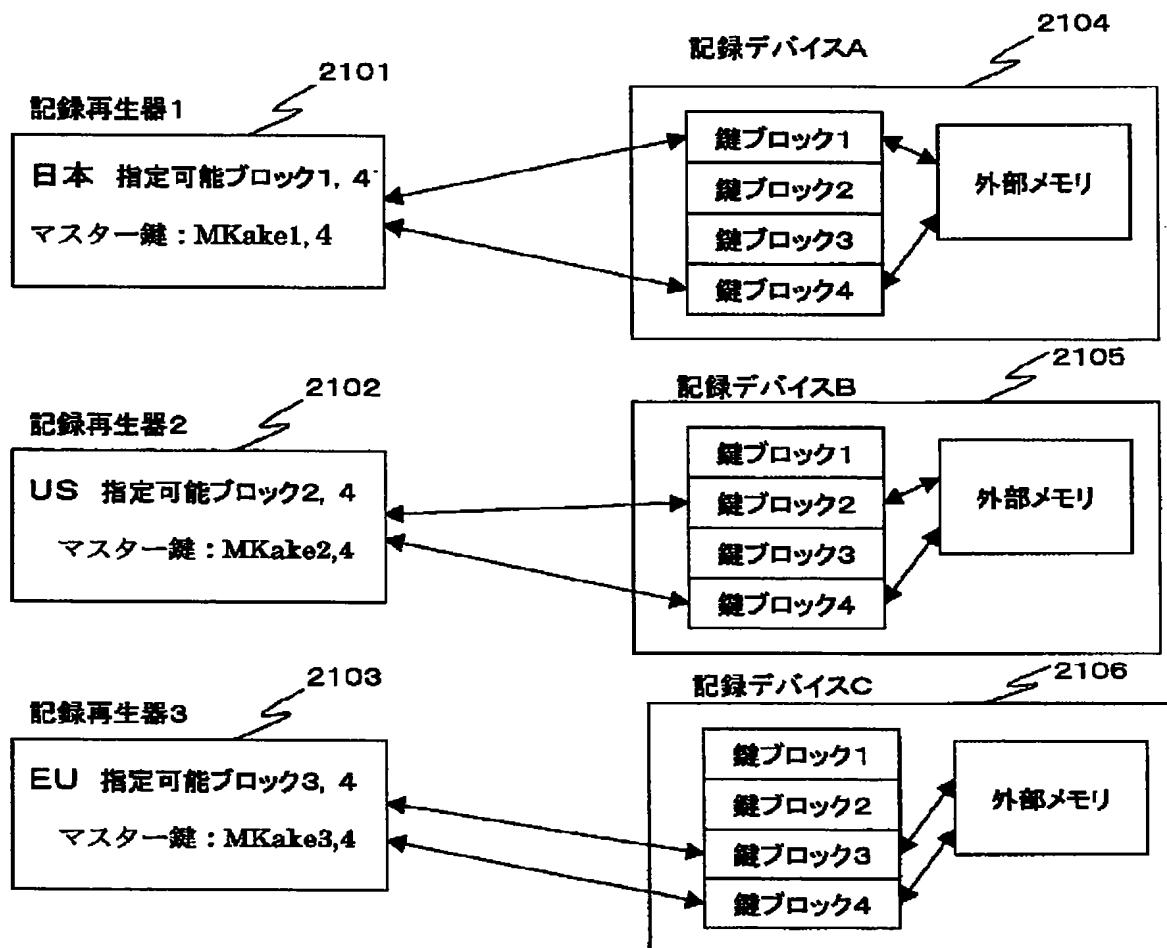
記録データ保持状況

【図20】

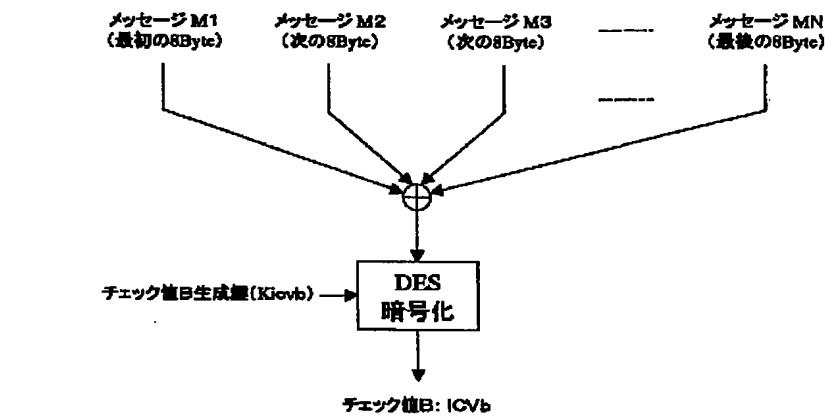


記録再生器と記録デバイスとの相互認証

【図21】



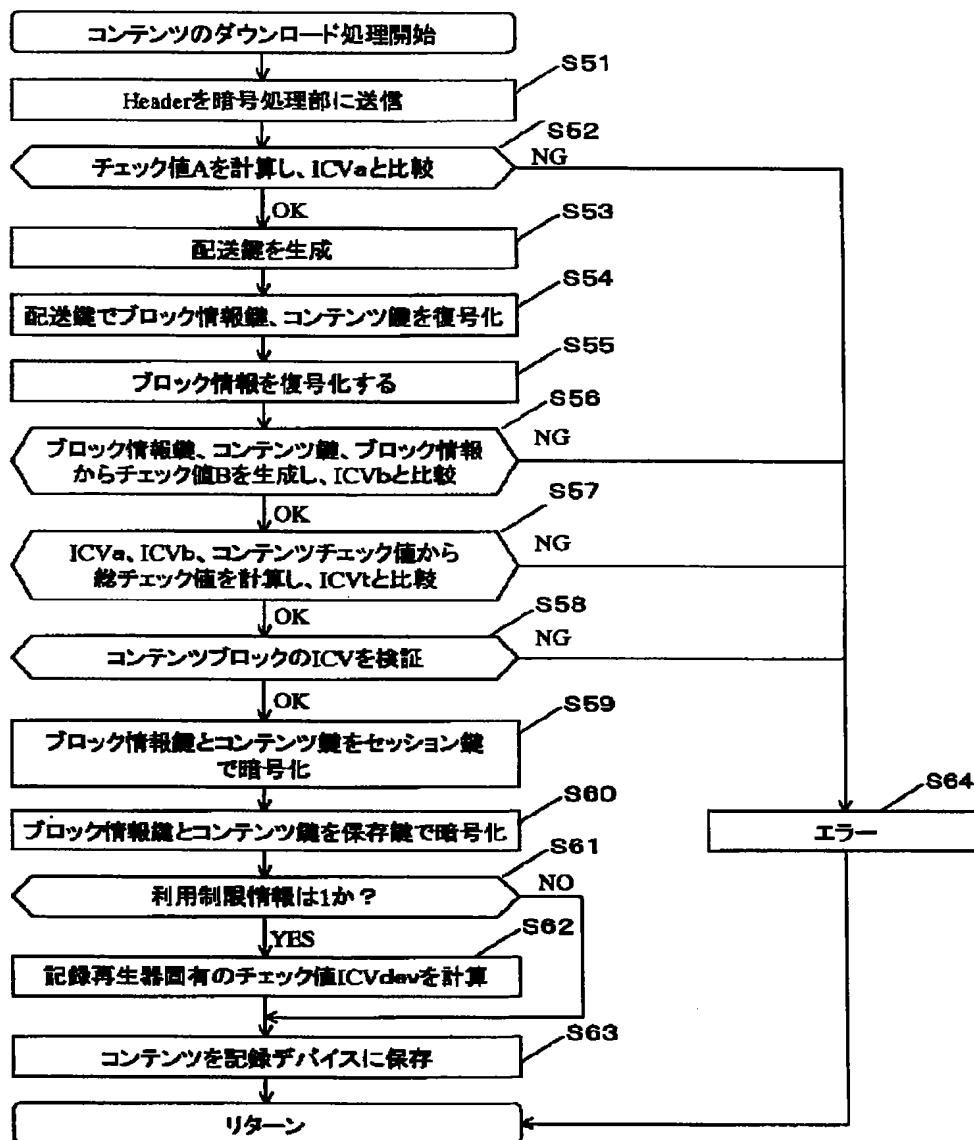
【図24】



メッセージ M1～MN: ブロック情報鍵Kbit, コンテンツ鍵Koon, ブロック情報

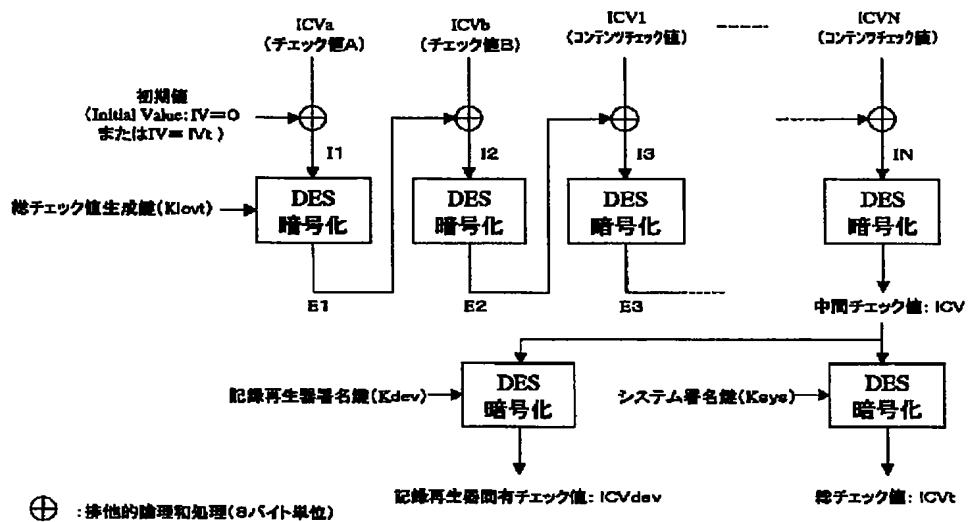
\oplus : 排他的論理和処理(8バイト単位)

【図22】

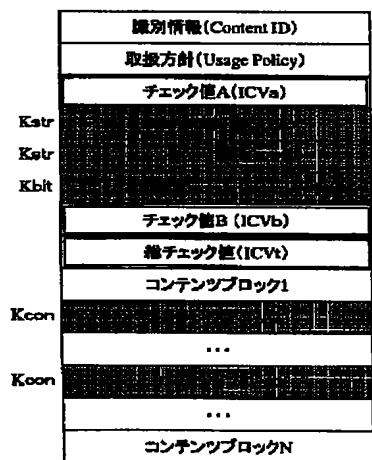


コンテンツのダウンロード処理

【図25】

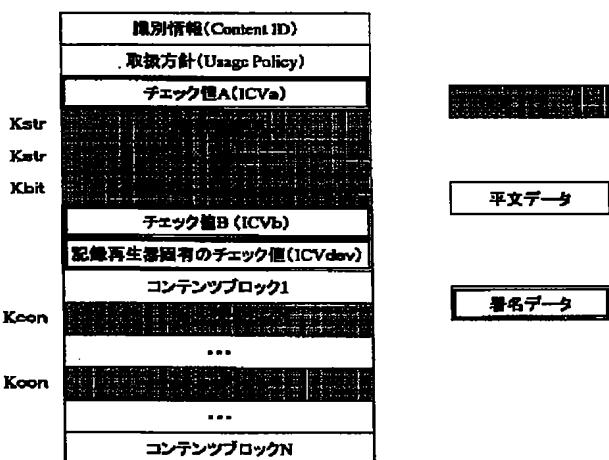


【図26】



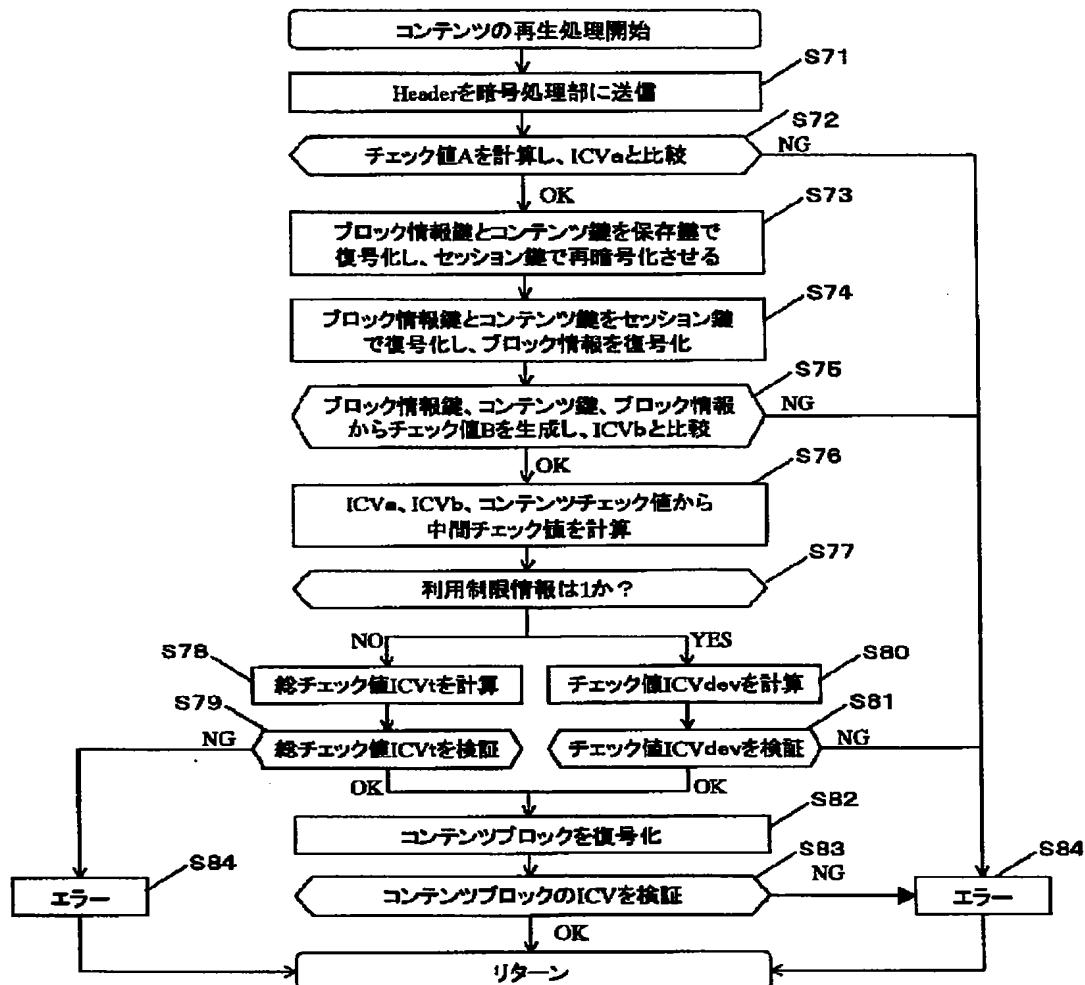
記録デバイスに保存されたコンテンツ
(利用制限情報=0)

【図27】

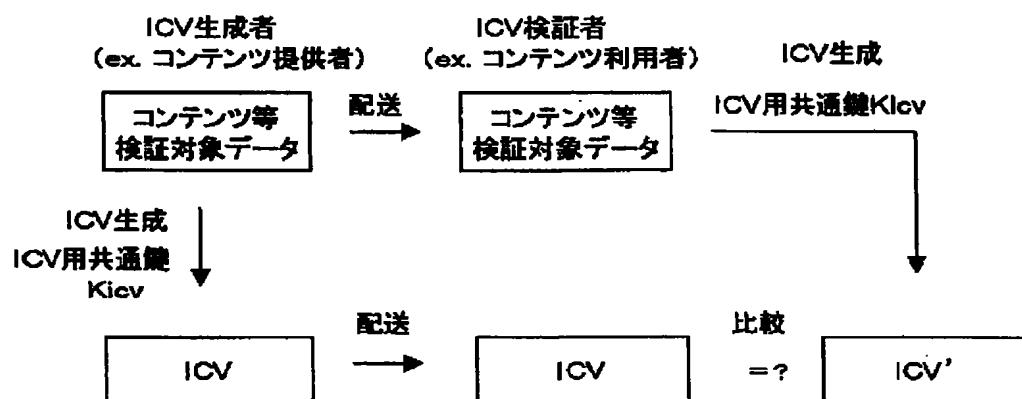


記録デバイスに保存されたコンテンツ
(利用制限情報=1)

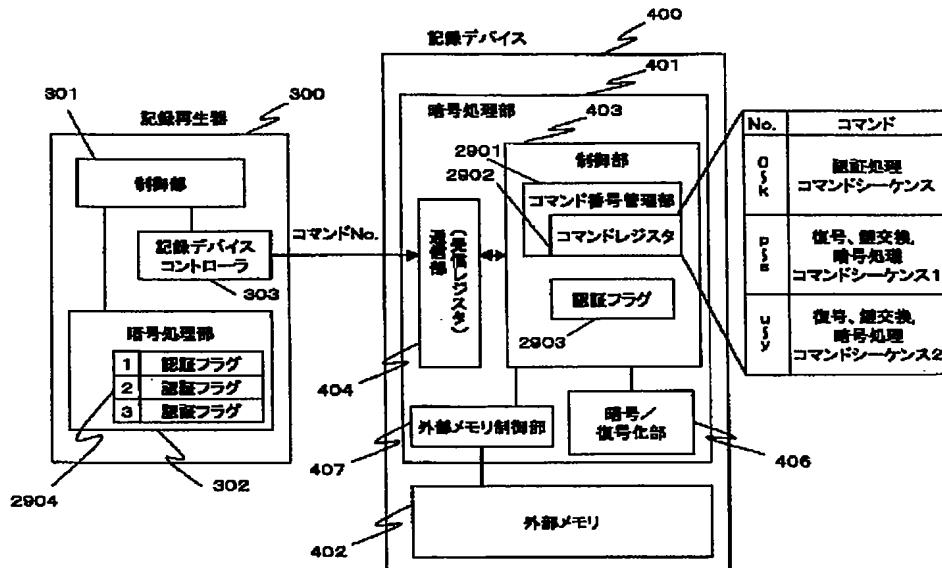
【図28】

コンテンツの再生処理

【図46】

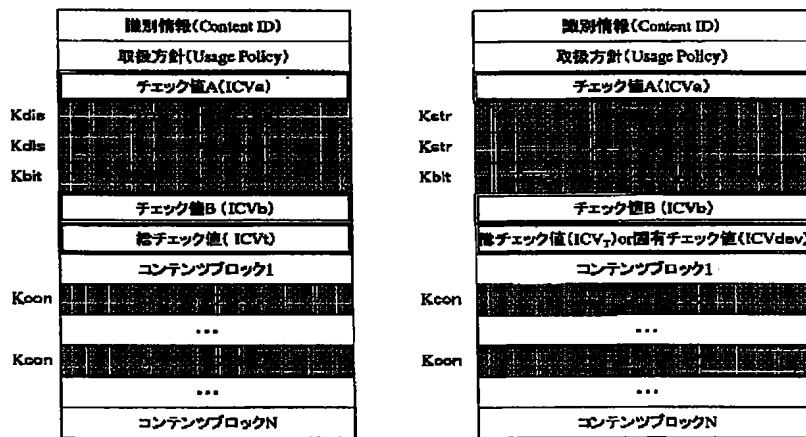


【図29】



【図32】

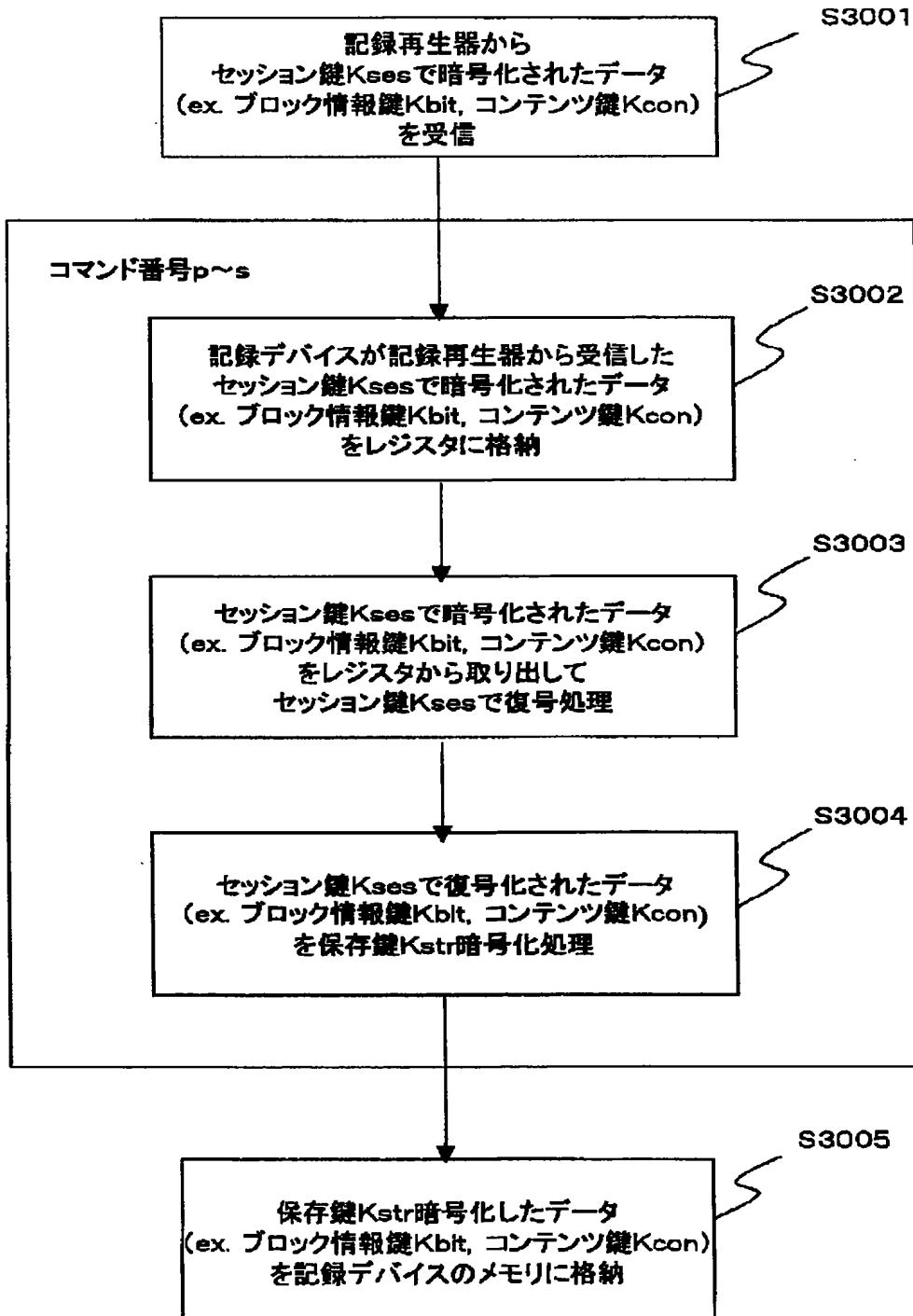
フォーマット・タイプ0



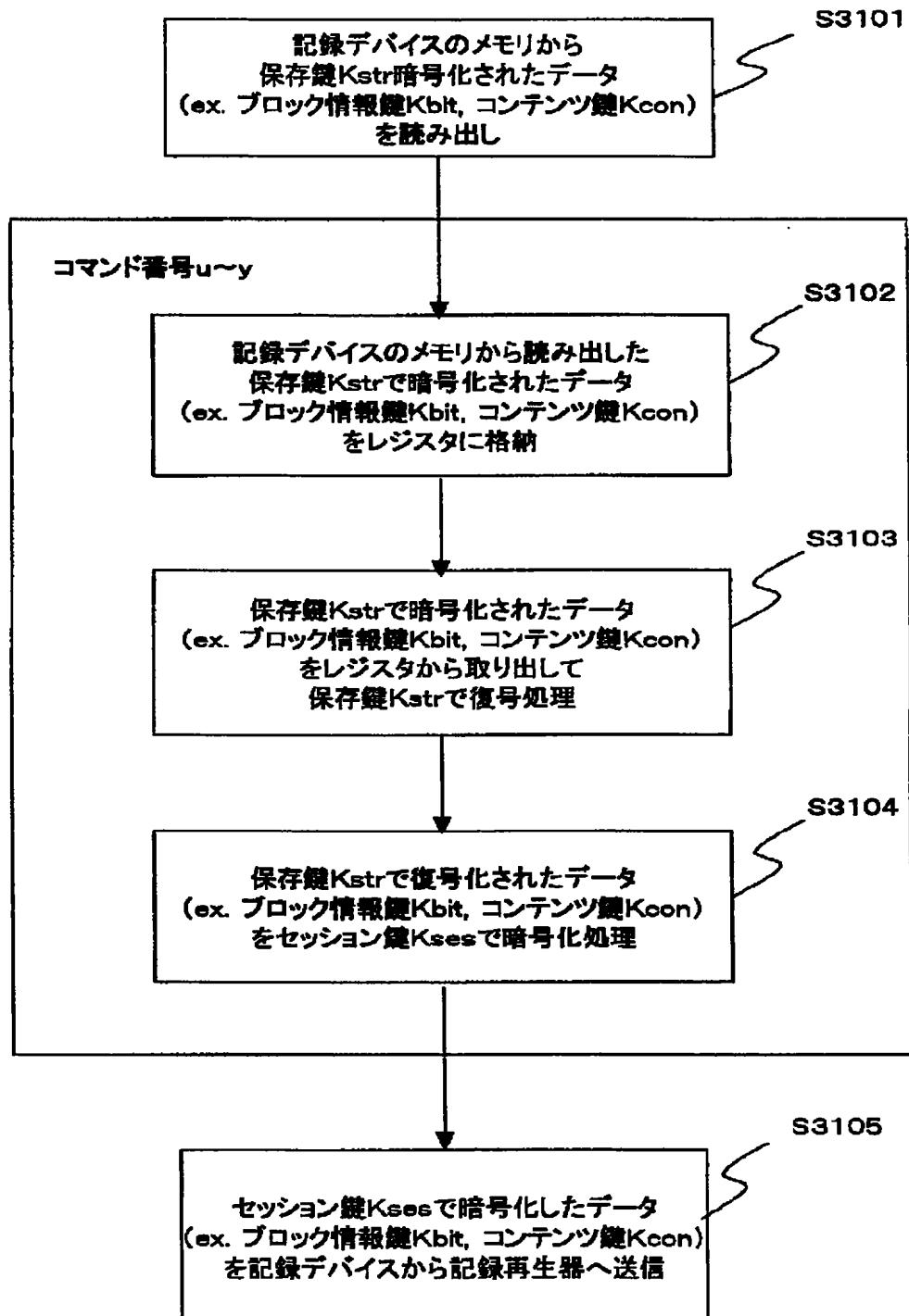
メディア上及び通信路上のデータフォーマット 記録デバイスに保存されたコンテンツ

データ	平文データ	署名データ
-----	-------	-------

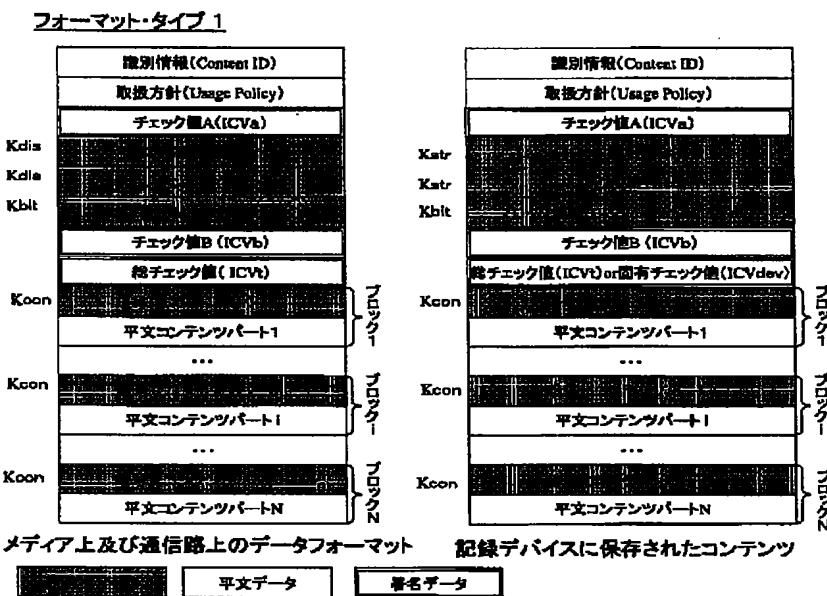
【図30】



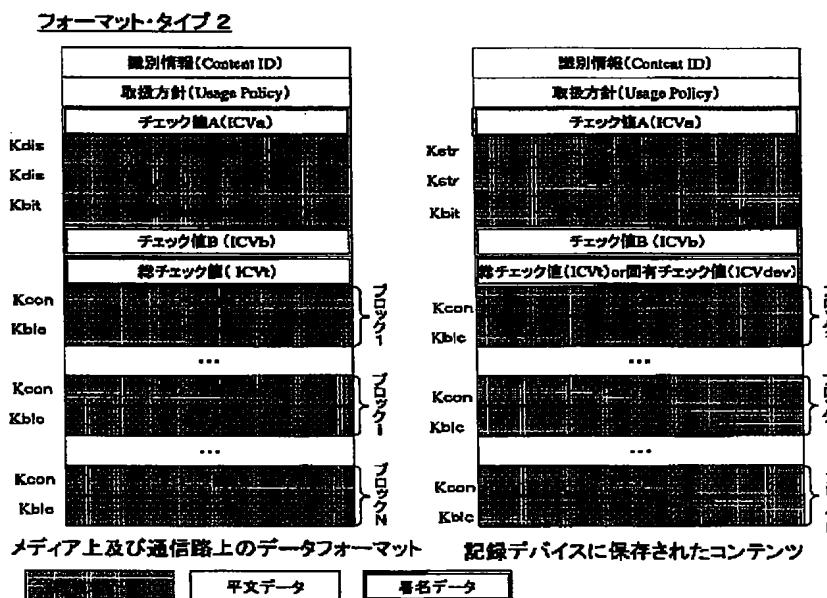
【図31】



【図33】

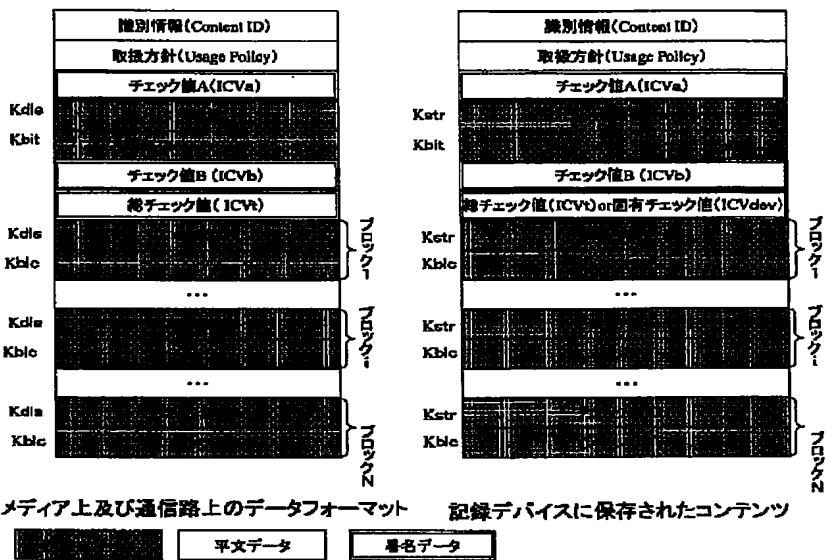


【図34】

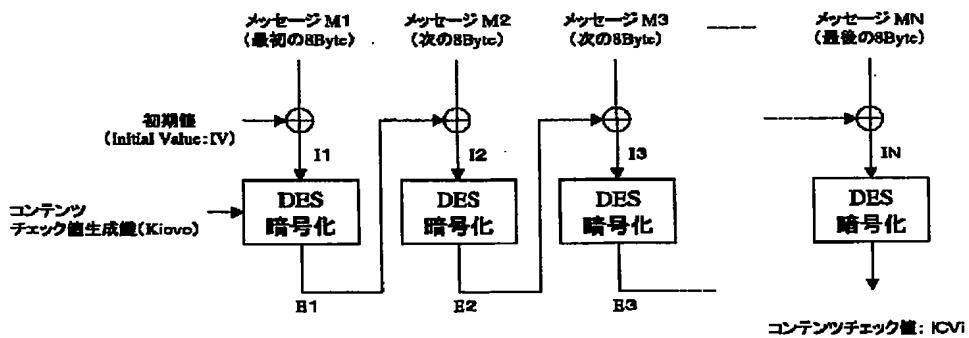


【図35】

フォーマット・タイプ3



【図36】

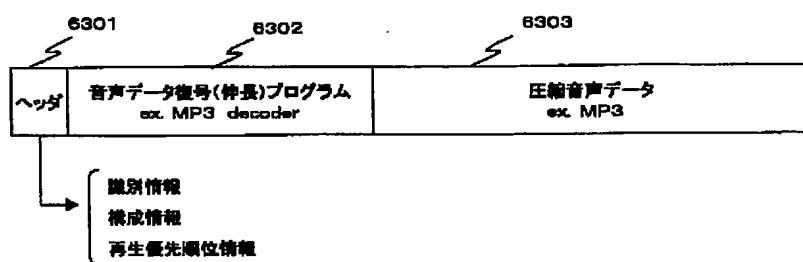


メッセージ M1～MN:コンテンツのコンテンツデータ

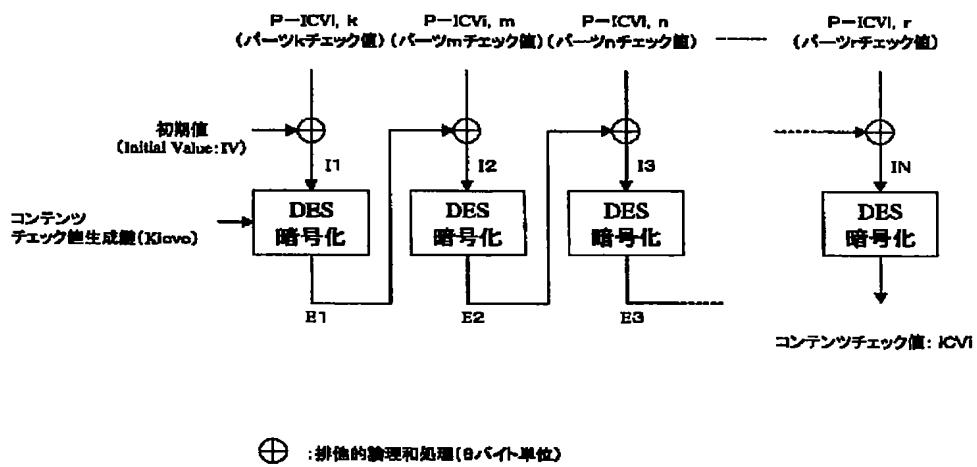
⊕ : 排他的論理和処理(8バイト単位)

【図65】

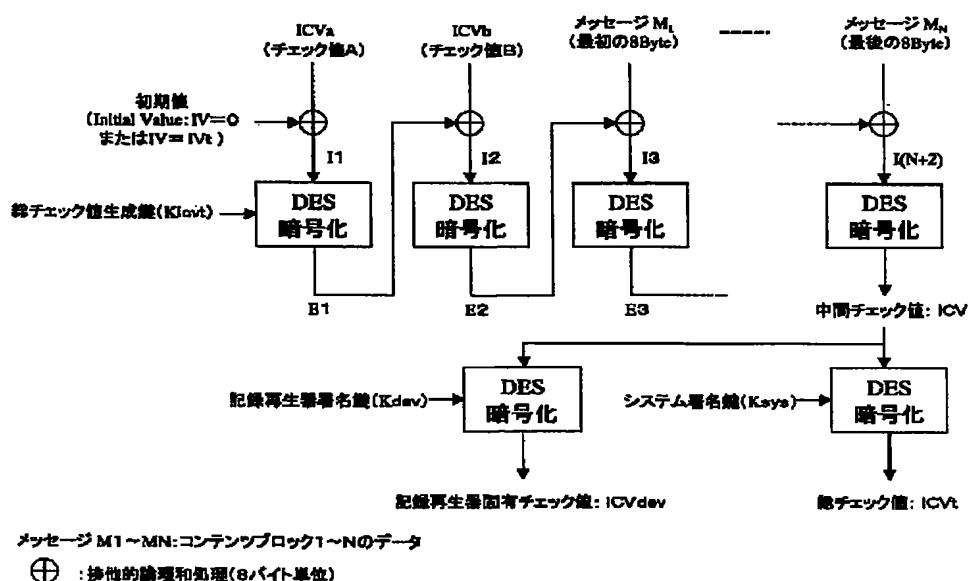
コンテンツ構成例(3)



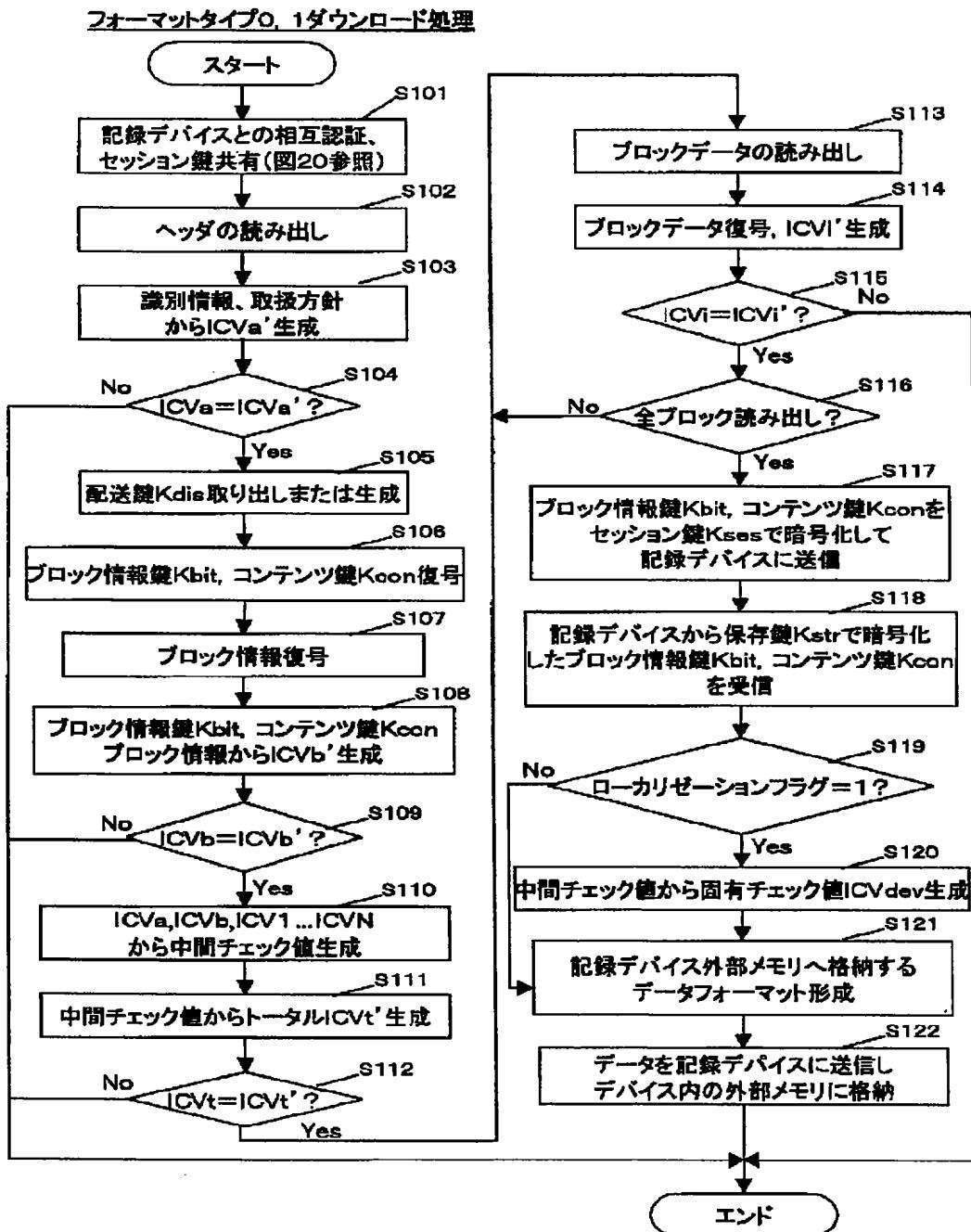
【図3.7】



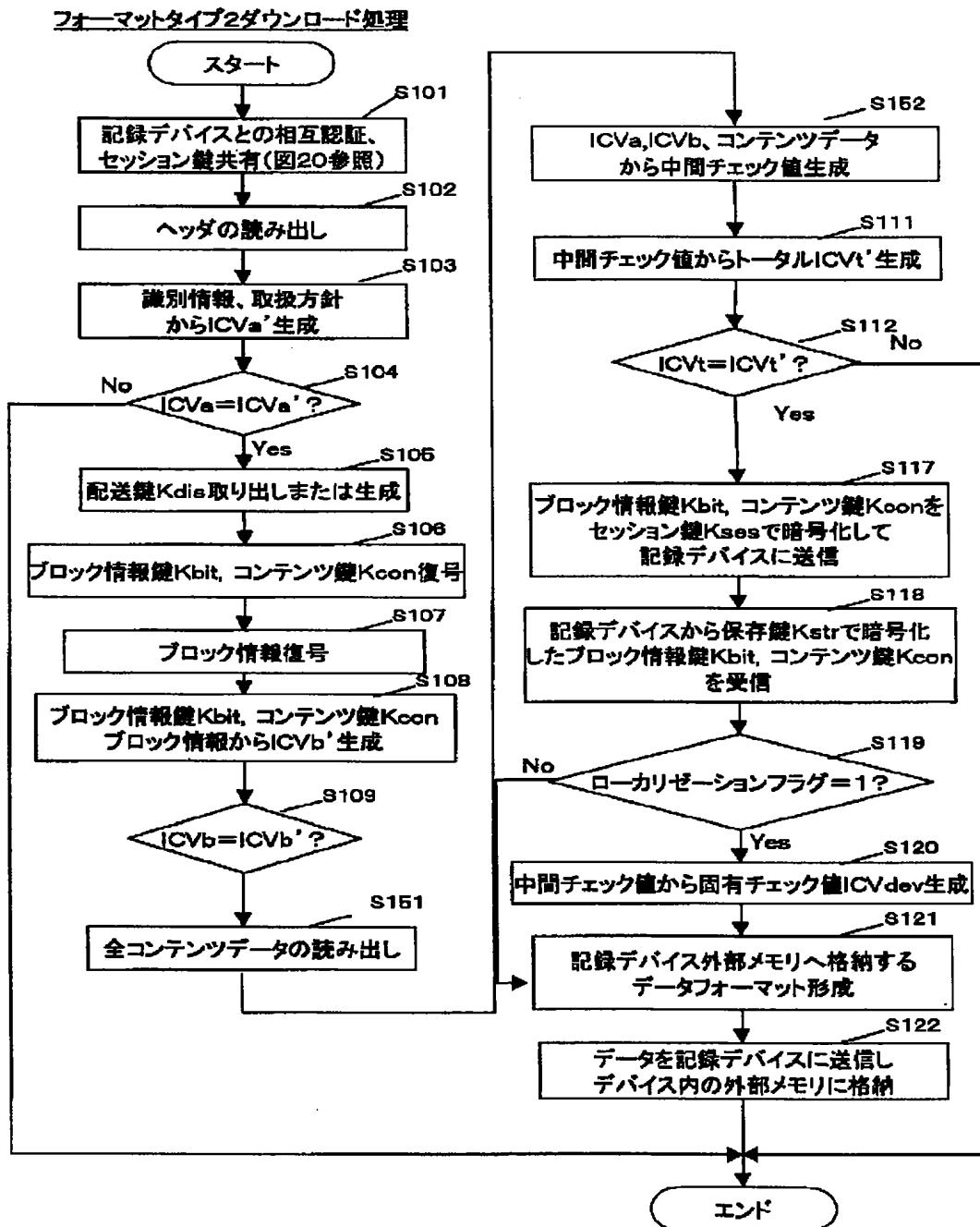
【図3.8】



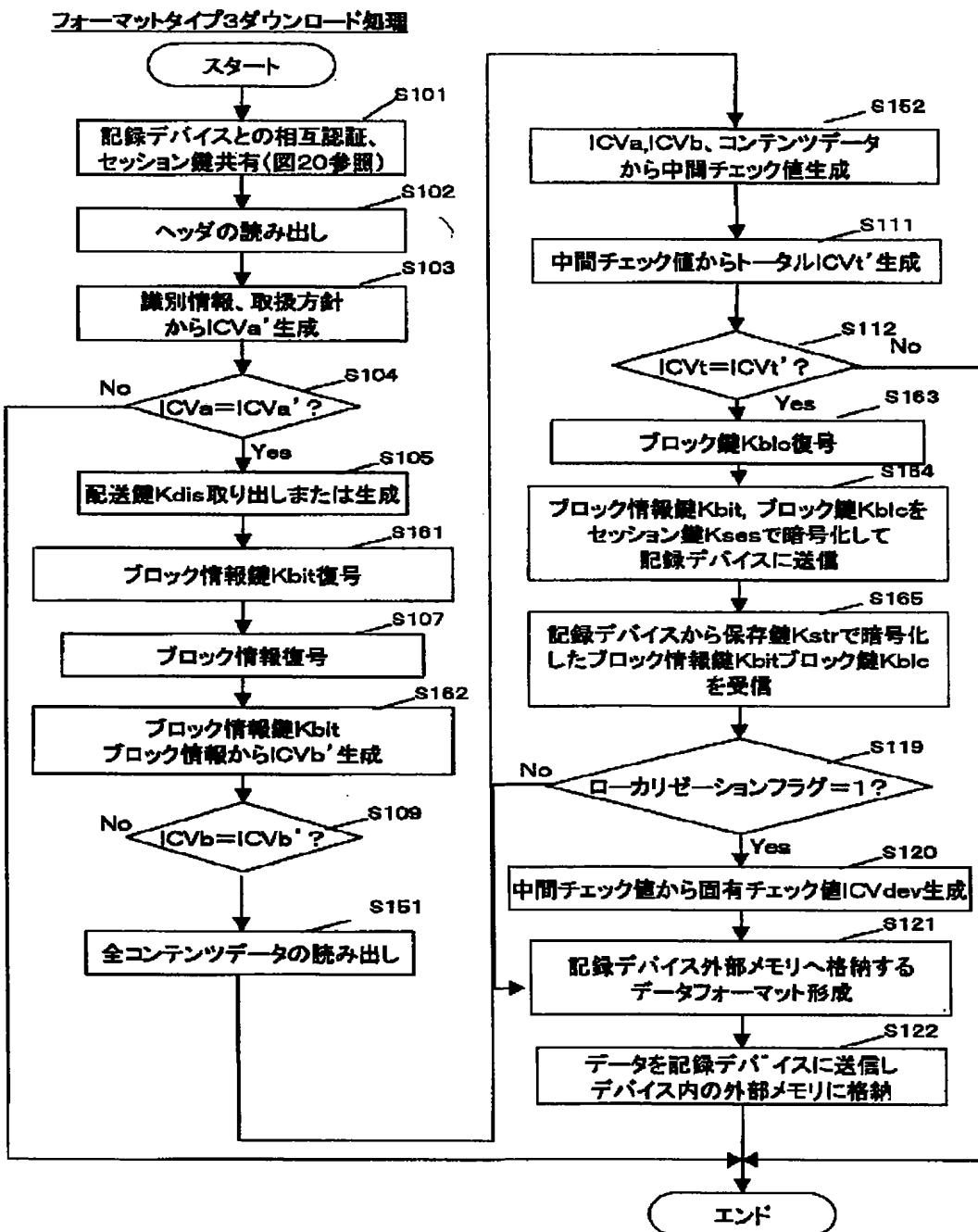
【図39】



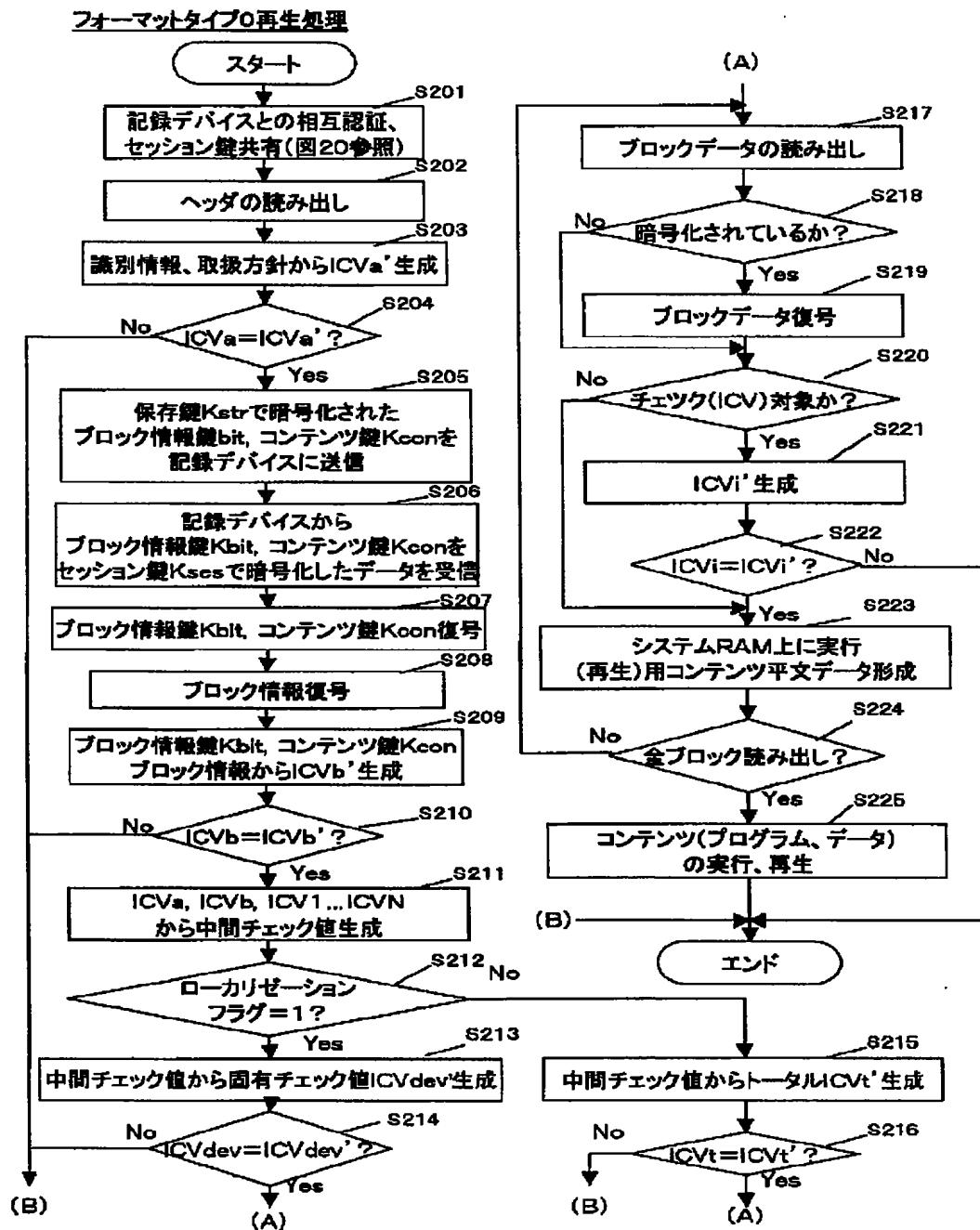
【図40】



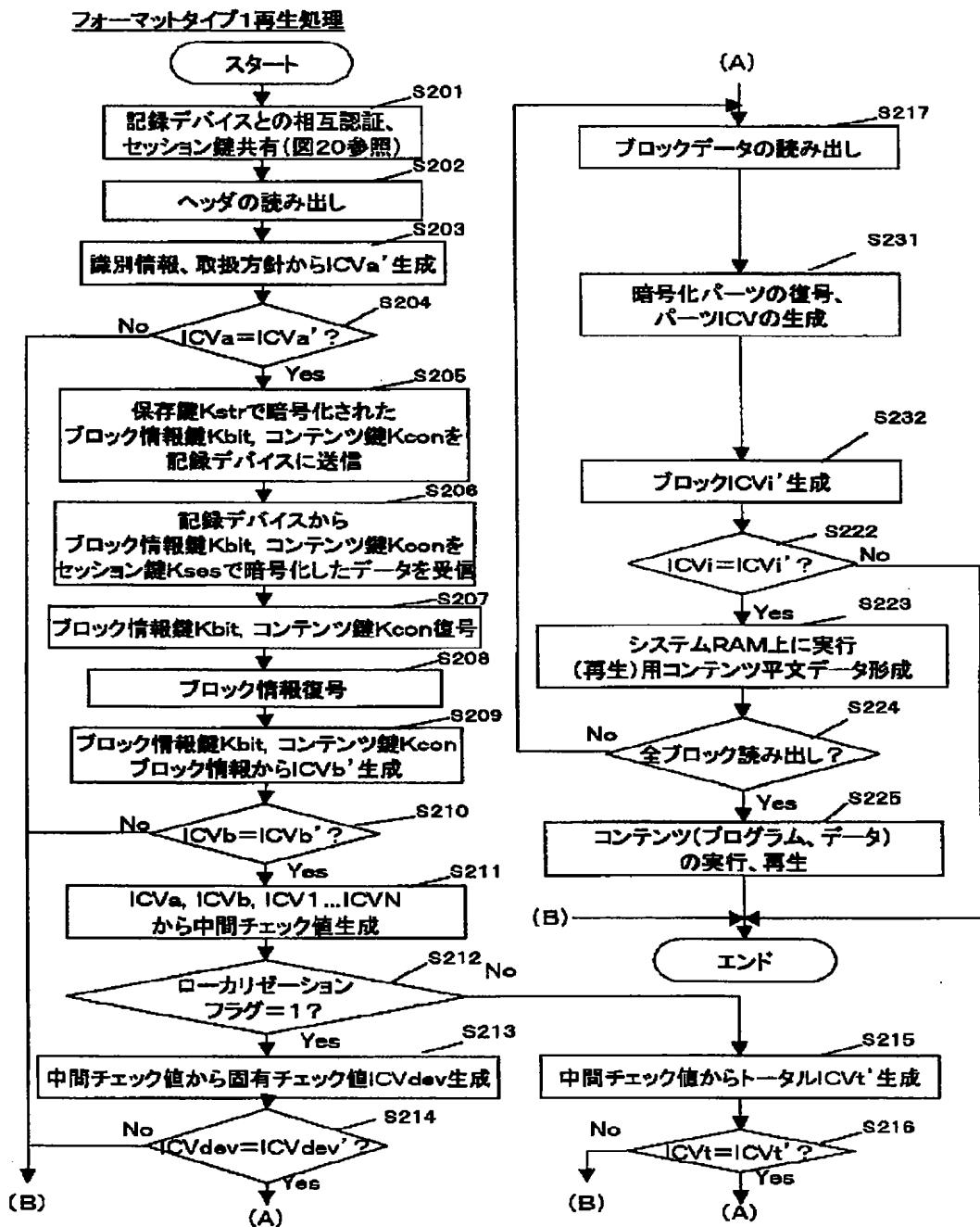
【図41】



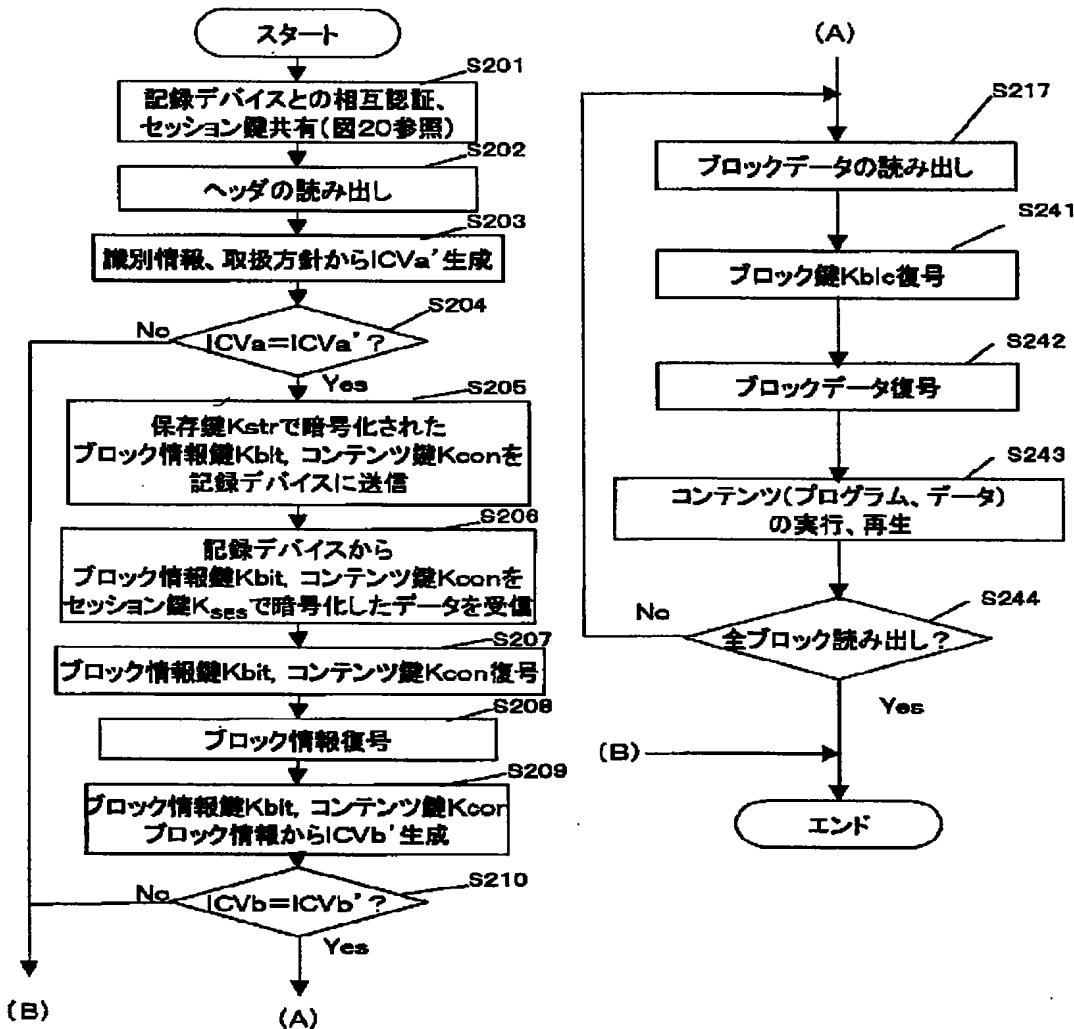
【図42】



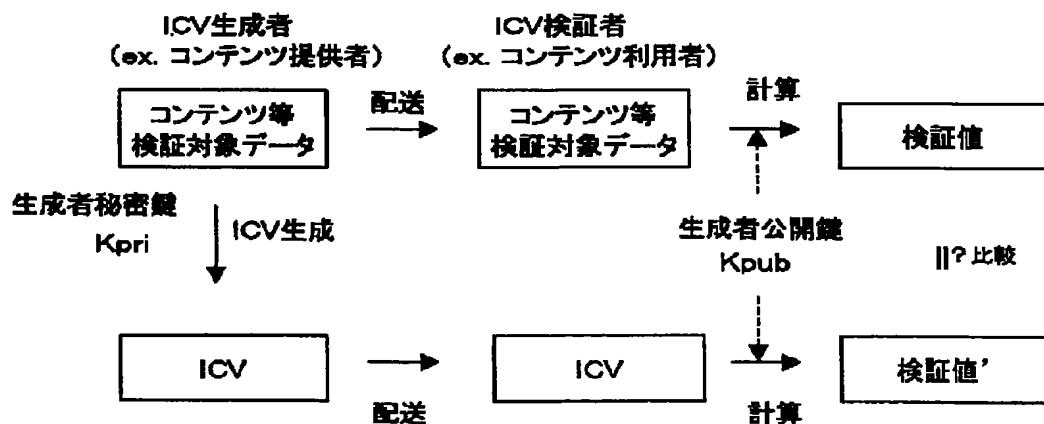
[図43]



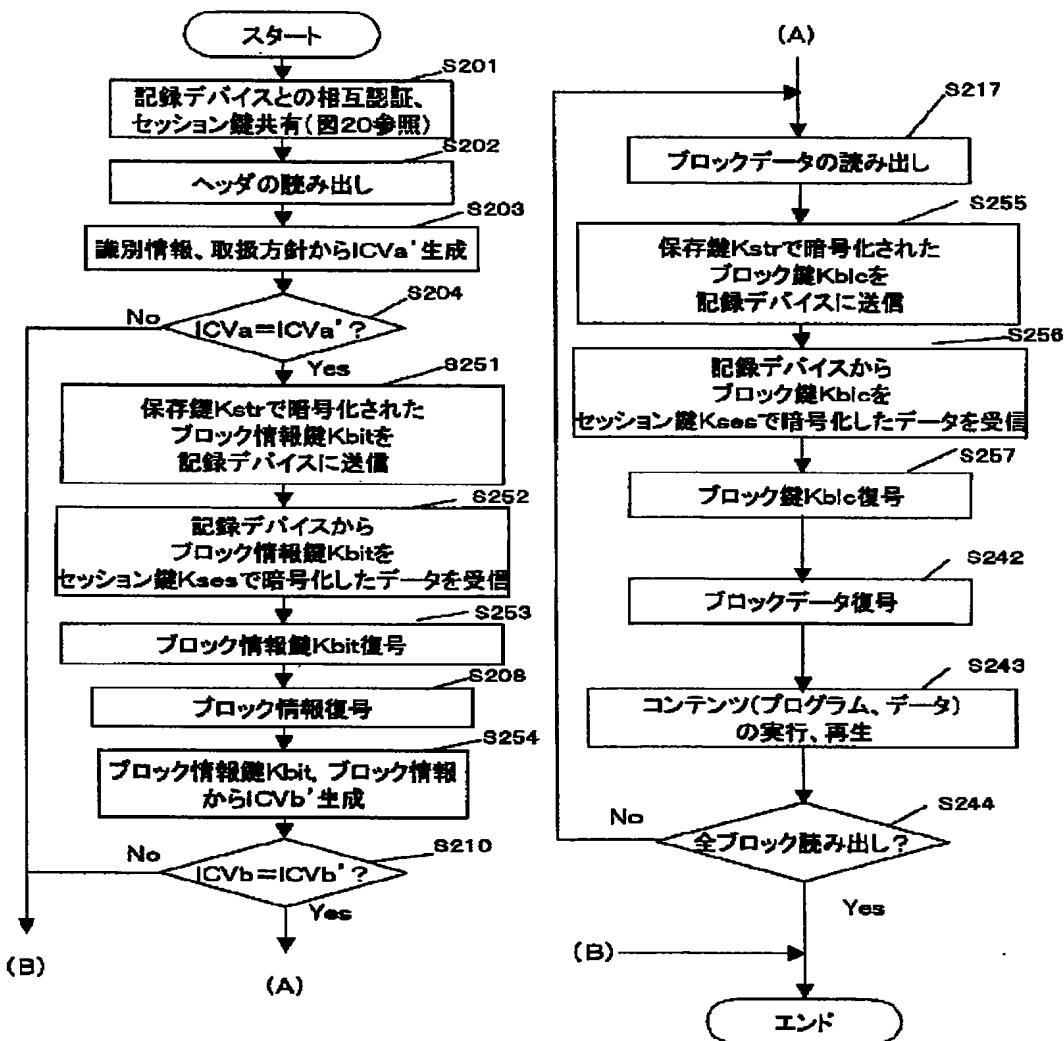
【図44】



【図47】

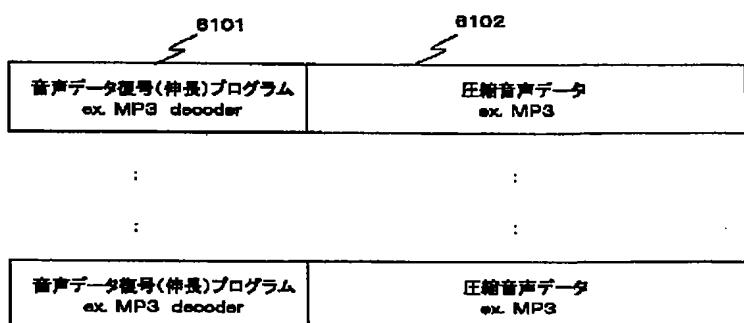


【図45】

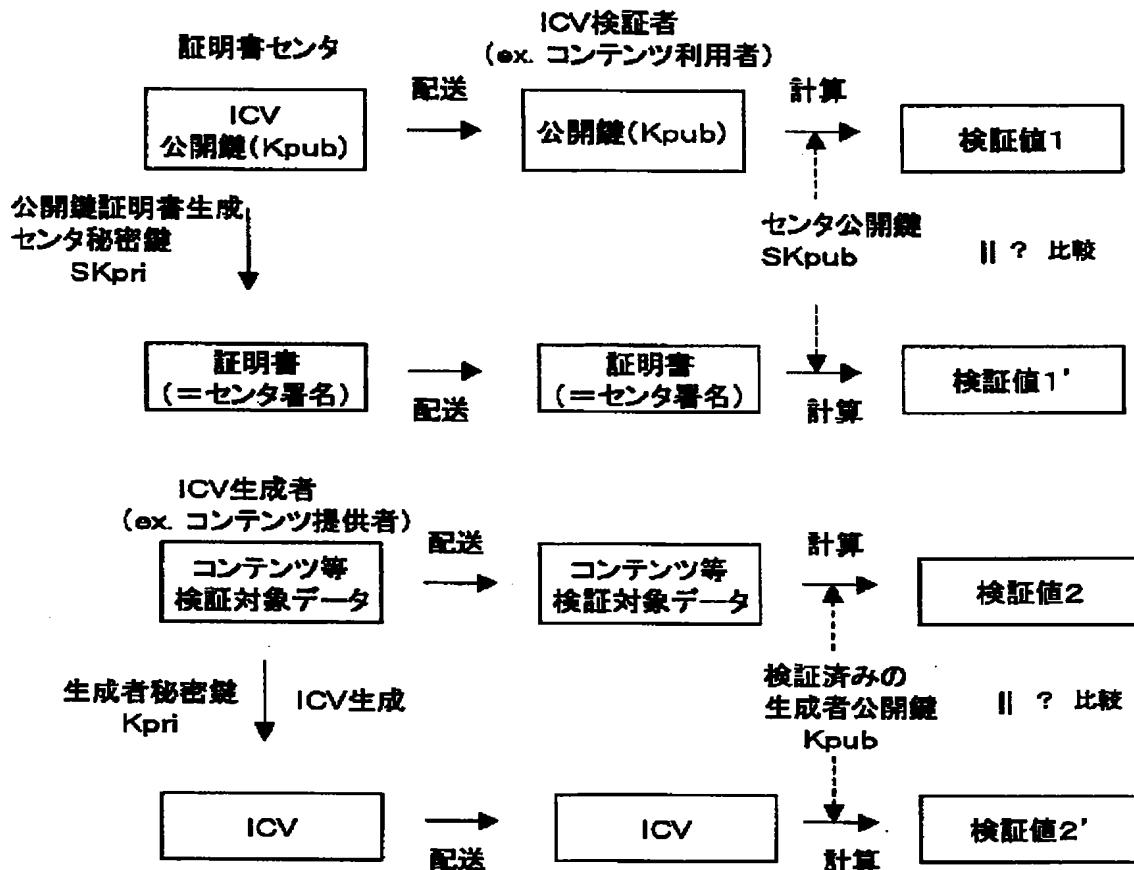
フォーマットタイプ3再生処理

【図61】

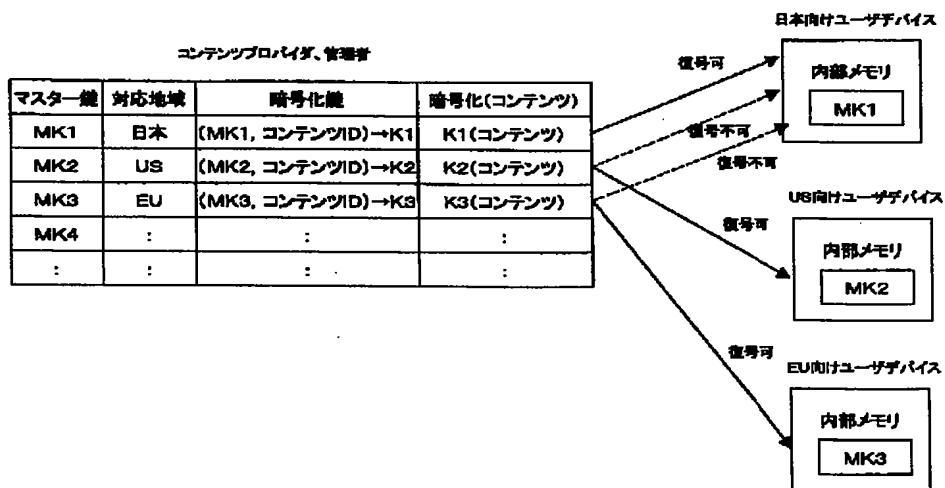
コンテンツ構成例(1)



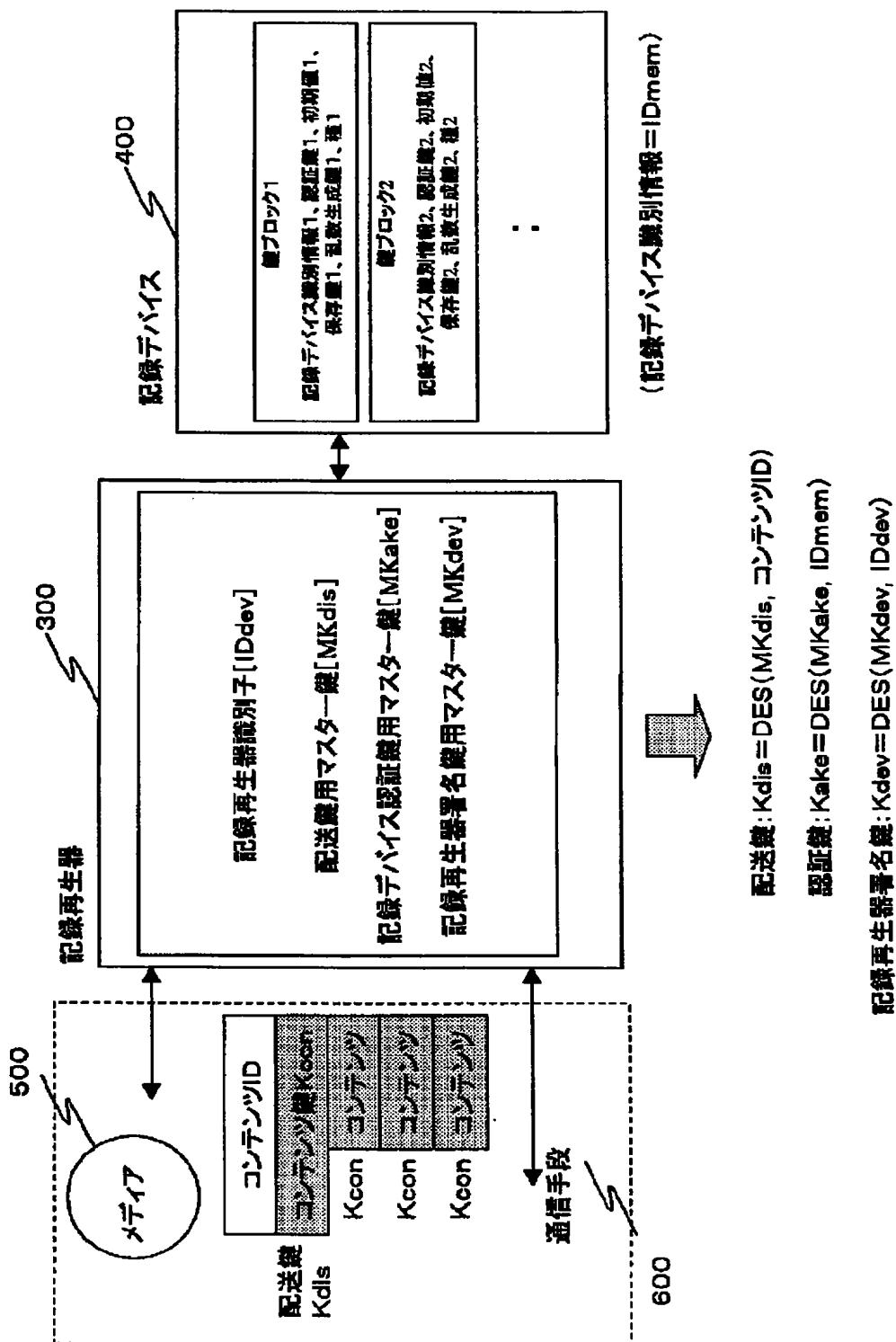
【図48】



【図52】



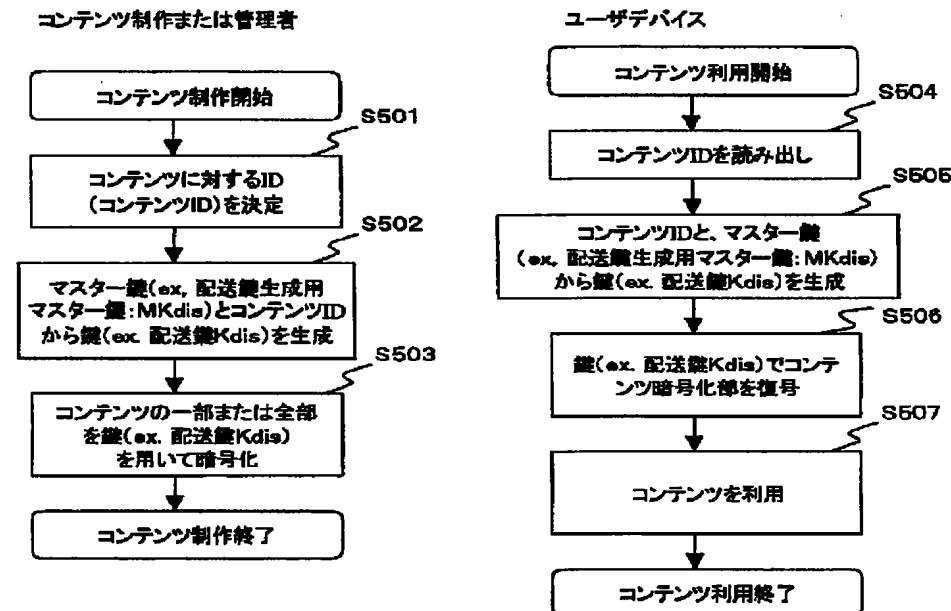
【図4.9】



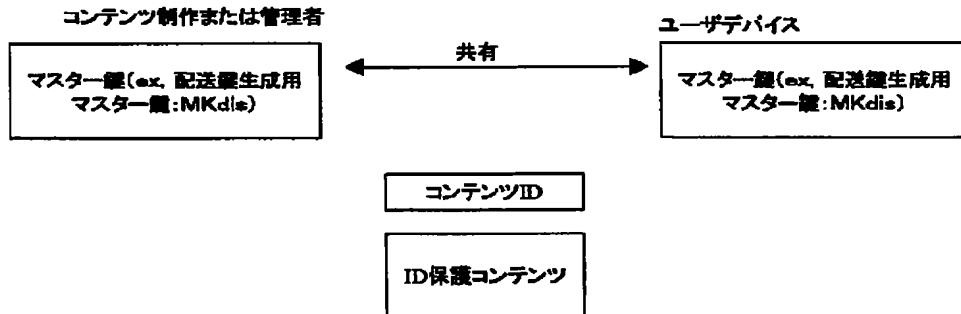
【図 5 0】

Master鍵から個別の鍵を生成する方法ー(1)

【基本フロー】



【鍵所有構成】



【図 7 1】

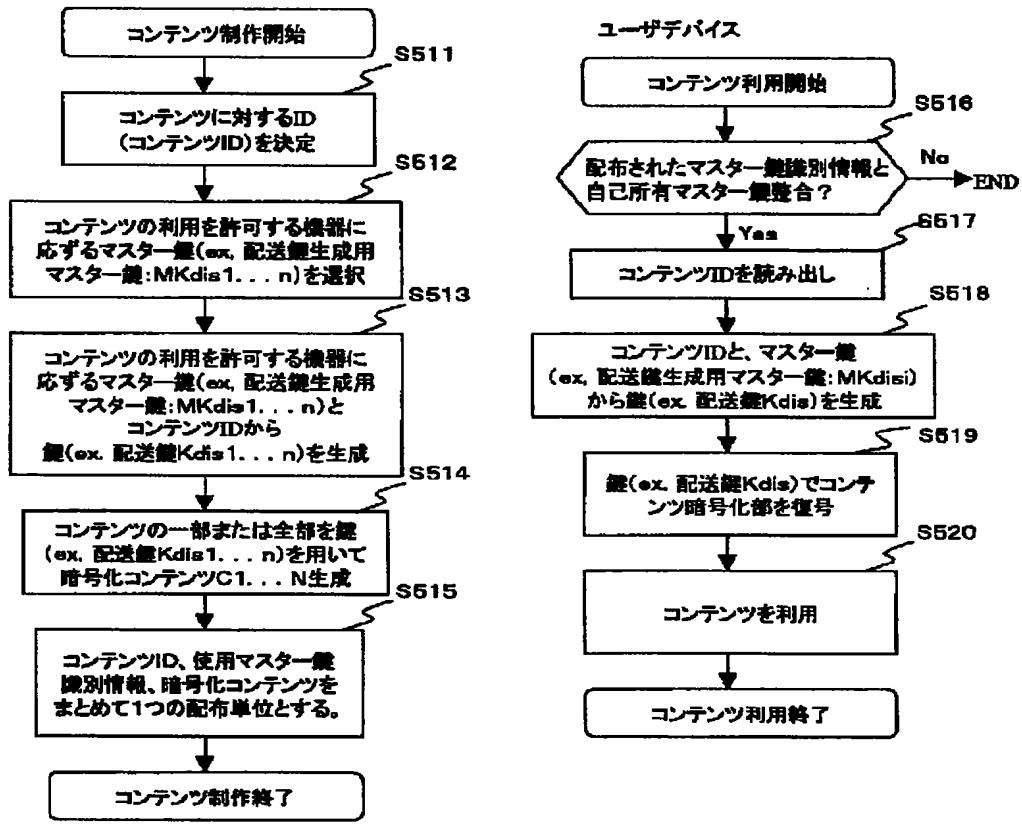
データ管理ファイル(1)

データ番号	コンテンツ識別子 (ゲームID)	記録再生器識別子 (IDdev)	プログラム使用制限
1	12345678...	56789012...	する
2	ABCDEF12...	09876543...	する
3	122457678...	58834762...	しない
:	:	:	:

【図51】

Master鍵から個別の鍵を生成する方法-(2)

[基本フロー]
コンテンツ制作または管理者



[鍵所有構成]

コンテンツ制作または管理者

マスター鍵セット(ex. 配送鍵生成用
マスター鍵: MKdis1...n)

ID保護コンテンツ

ユーザデバイス

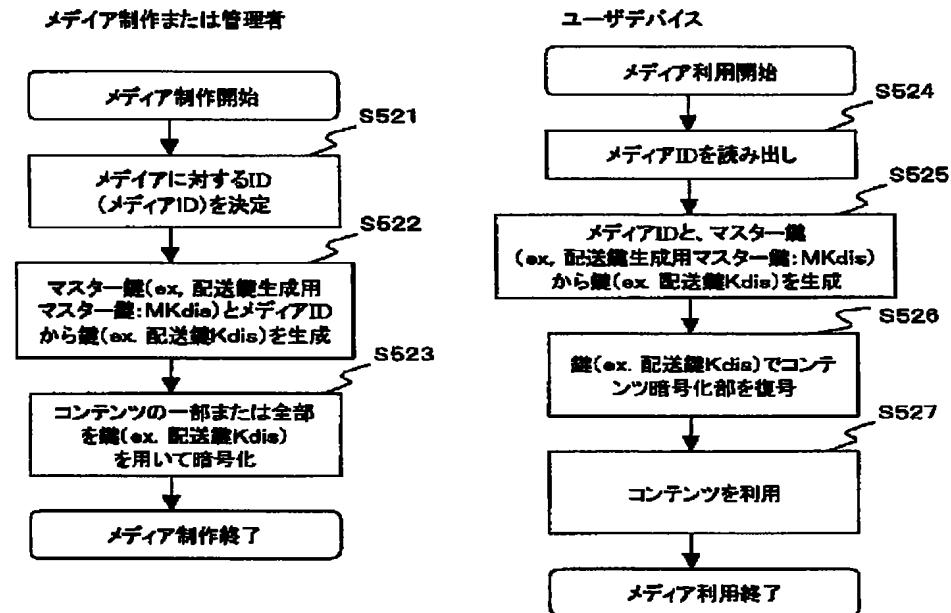
マスター鍵(ex. 配送鍵生成用
マスター鍵: MKdisi)

共有

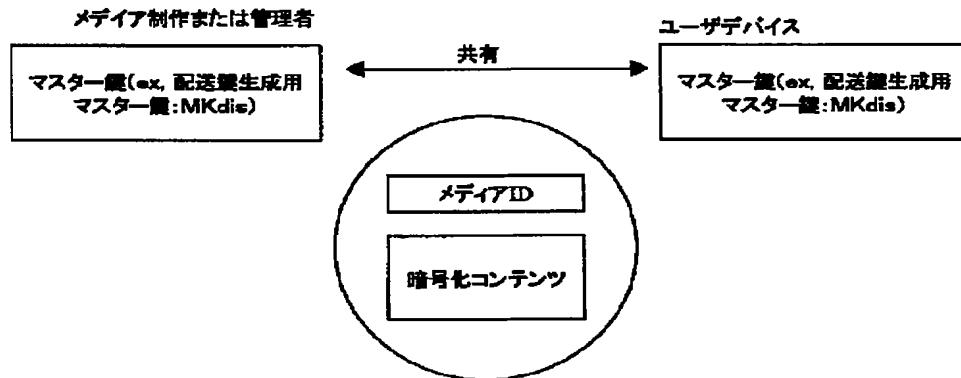
【図53】

Master鍵から個別の鍵を生成する方法ー(3)

【基本フロー】



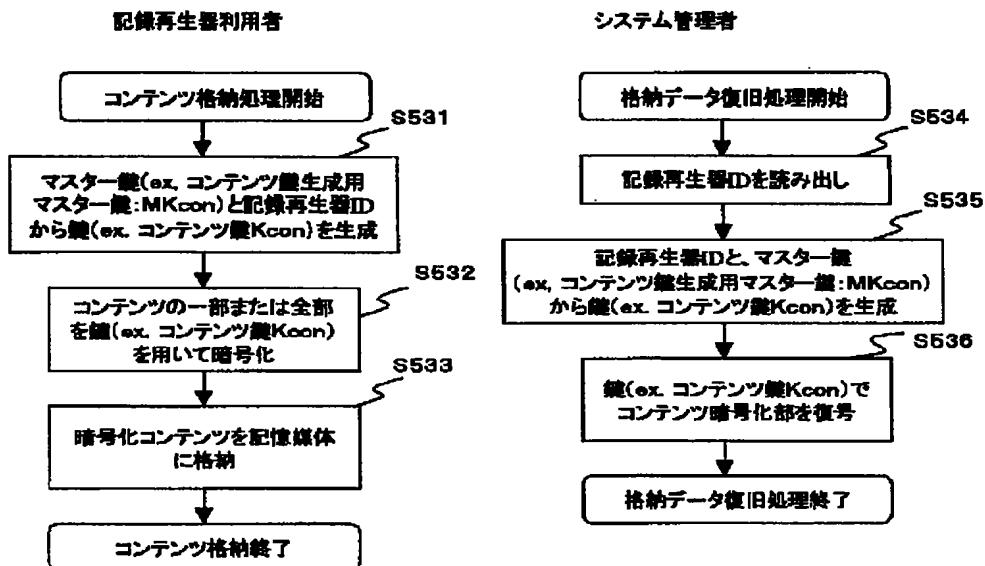
【鍵所有構成】



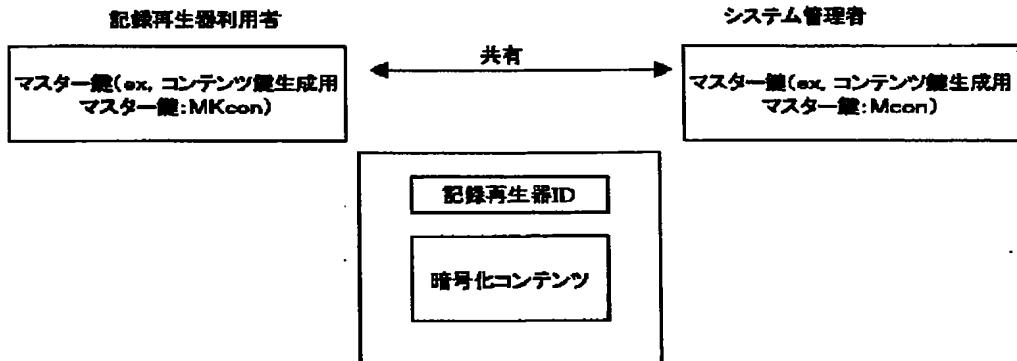
【図54】

Master鍵から個別の鍵を生成する方法ー(4)

[基本フロー]



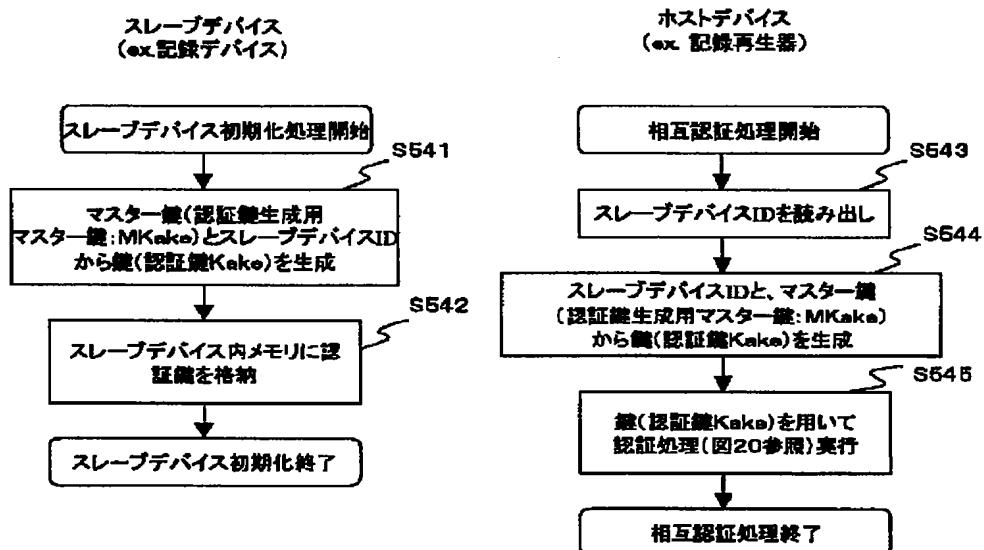
[鍵所有構成]



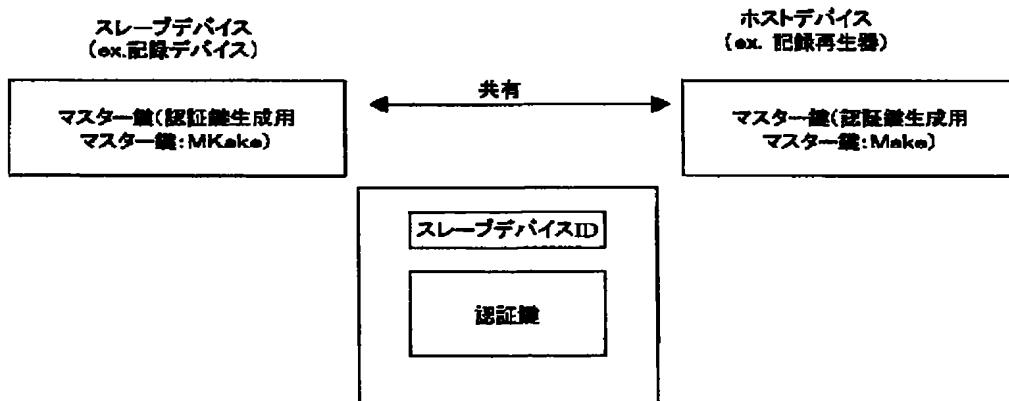
【図55】

Master鍵から個別の鍵を生成する方法ー(5)

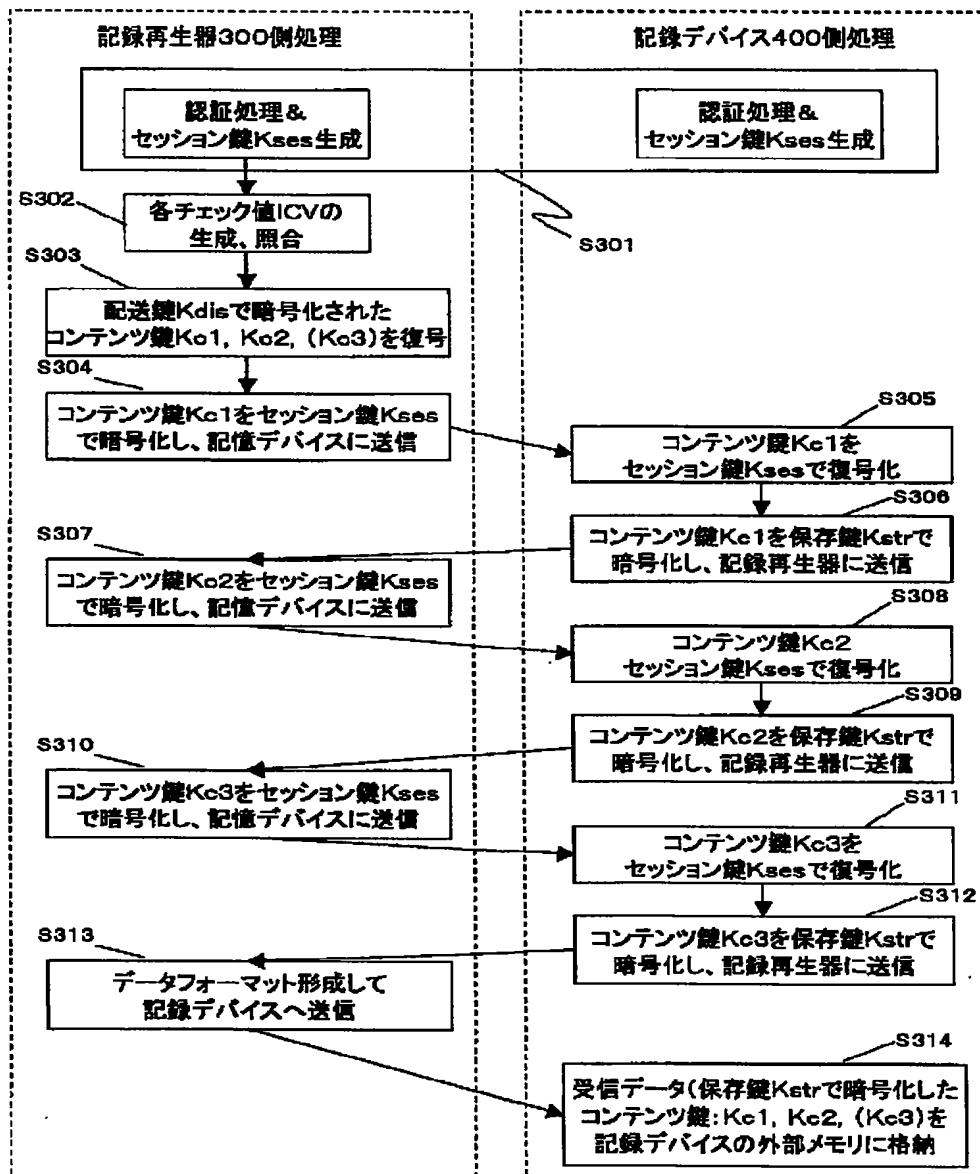
【基本フロー】



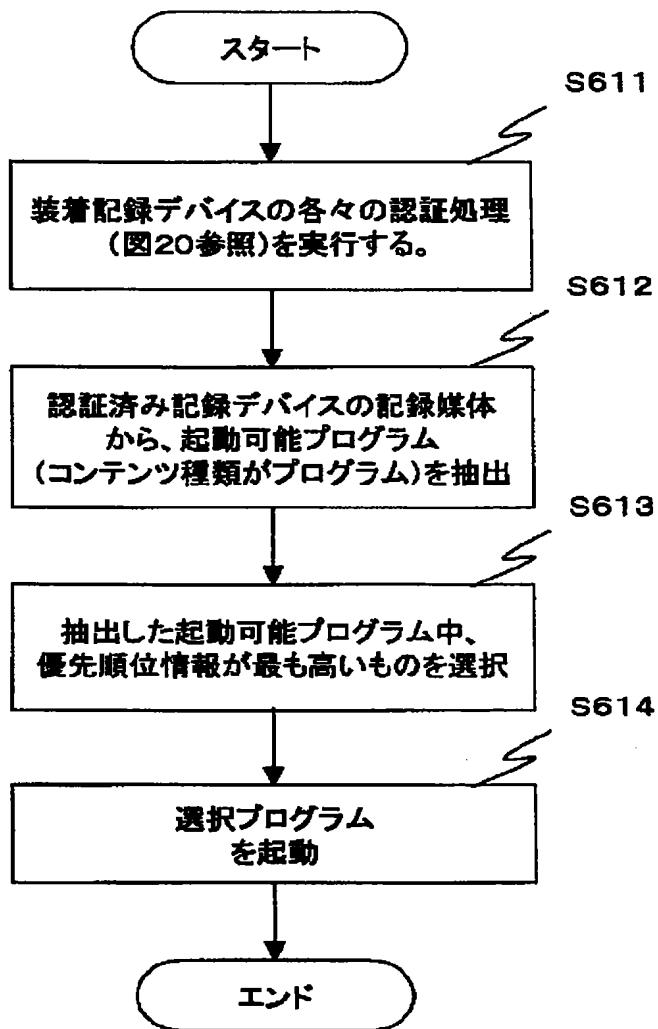
【鍵所有構成】



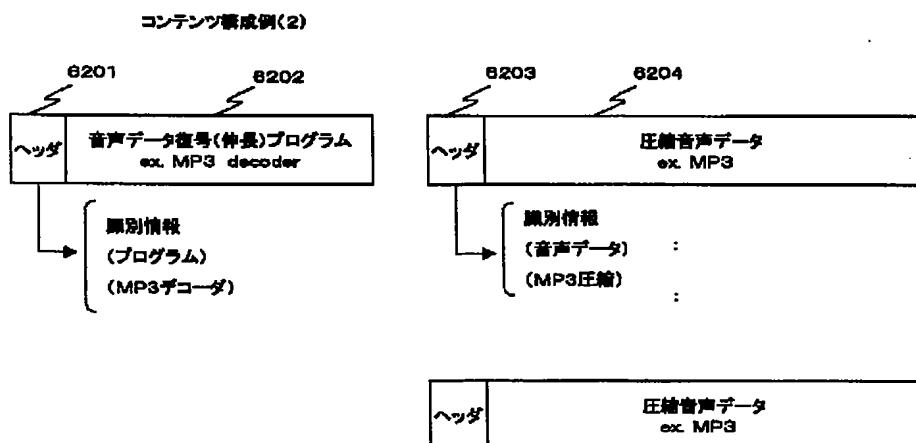
【図56】

トリプルDES適用コンテンツ鍵: $K_{c1}, K_{c2}, (K_{c3})$ の格納(ダウンロード)処理

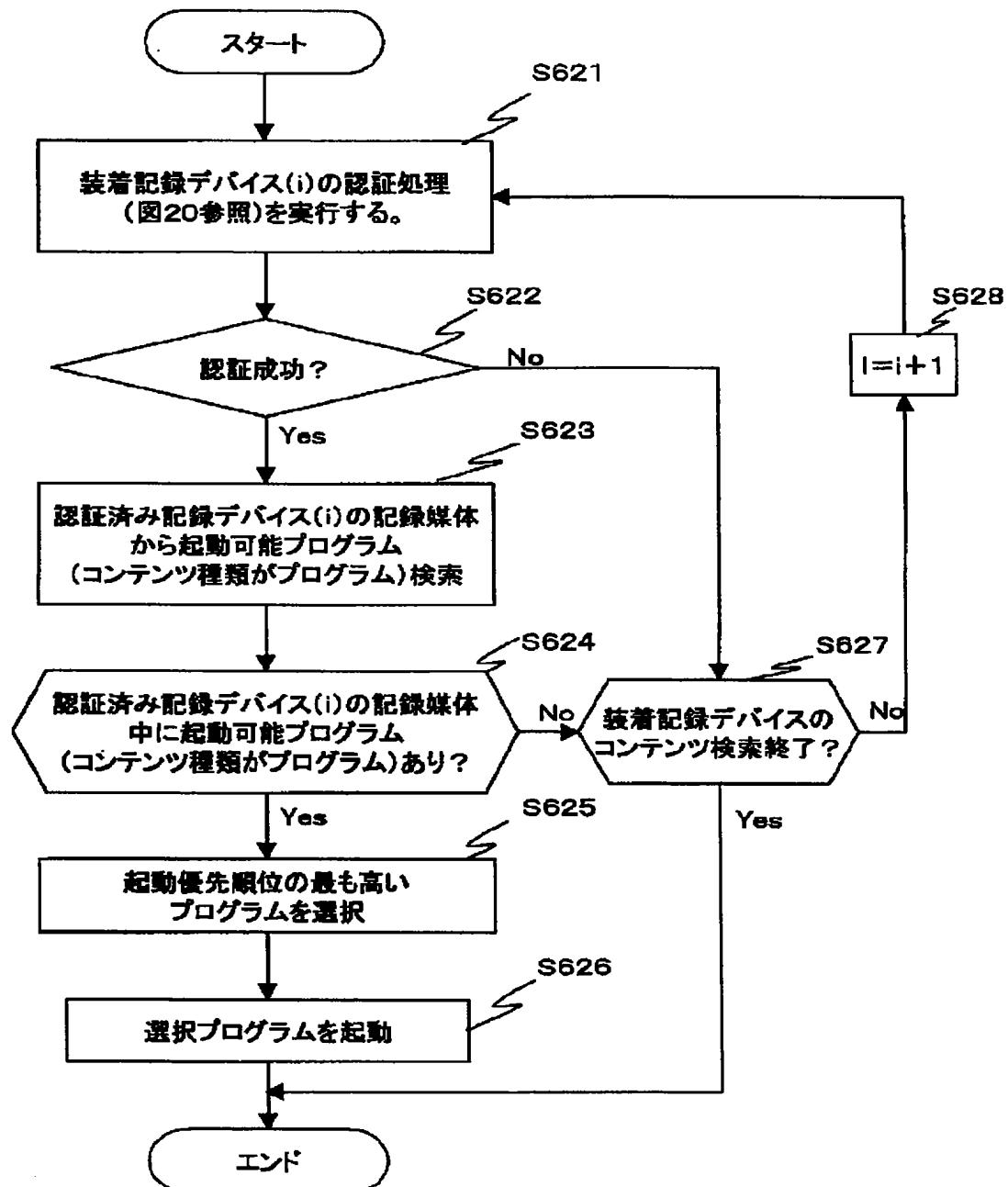
【図57】



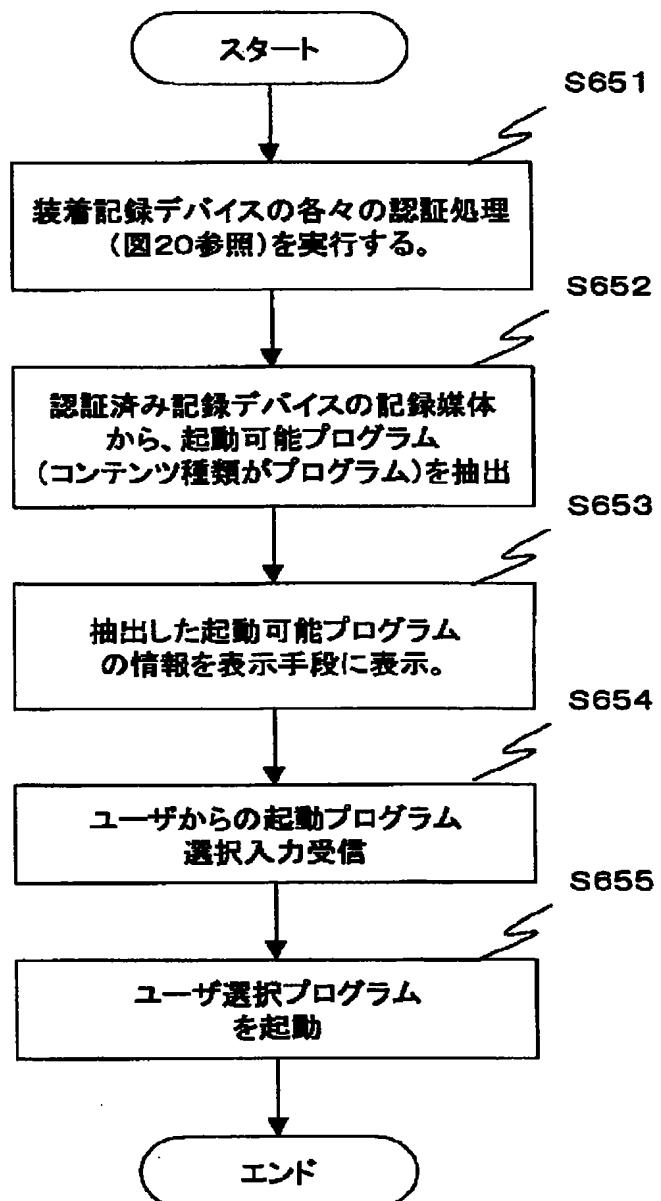
【図63】



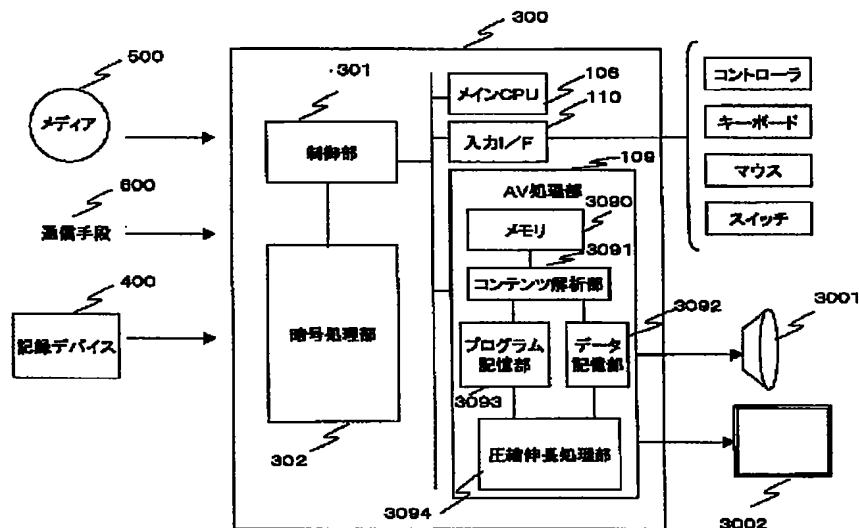
【図58】



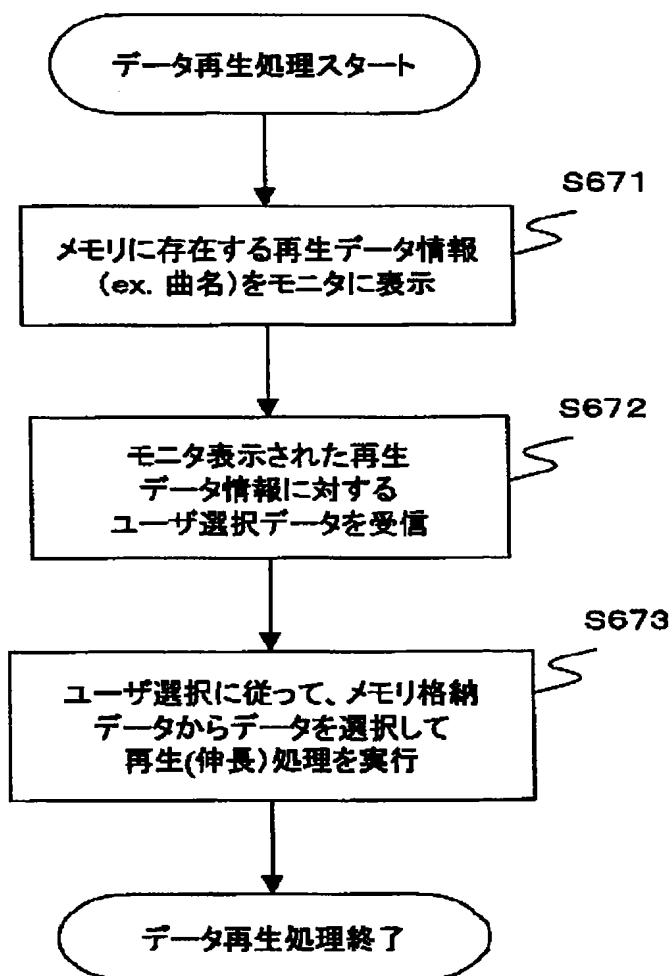
【図59】



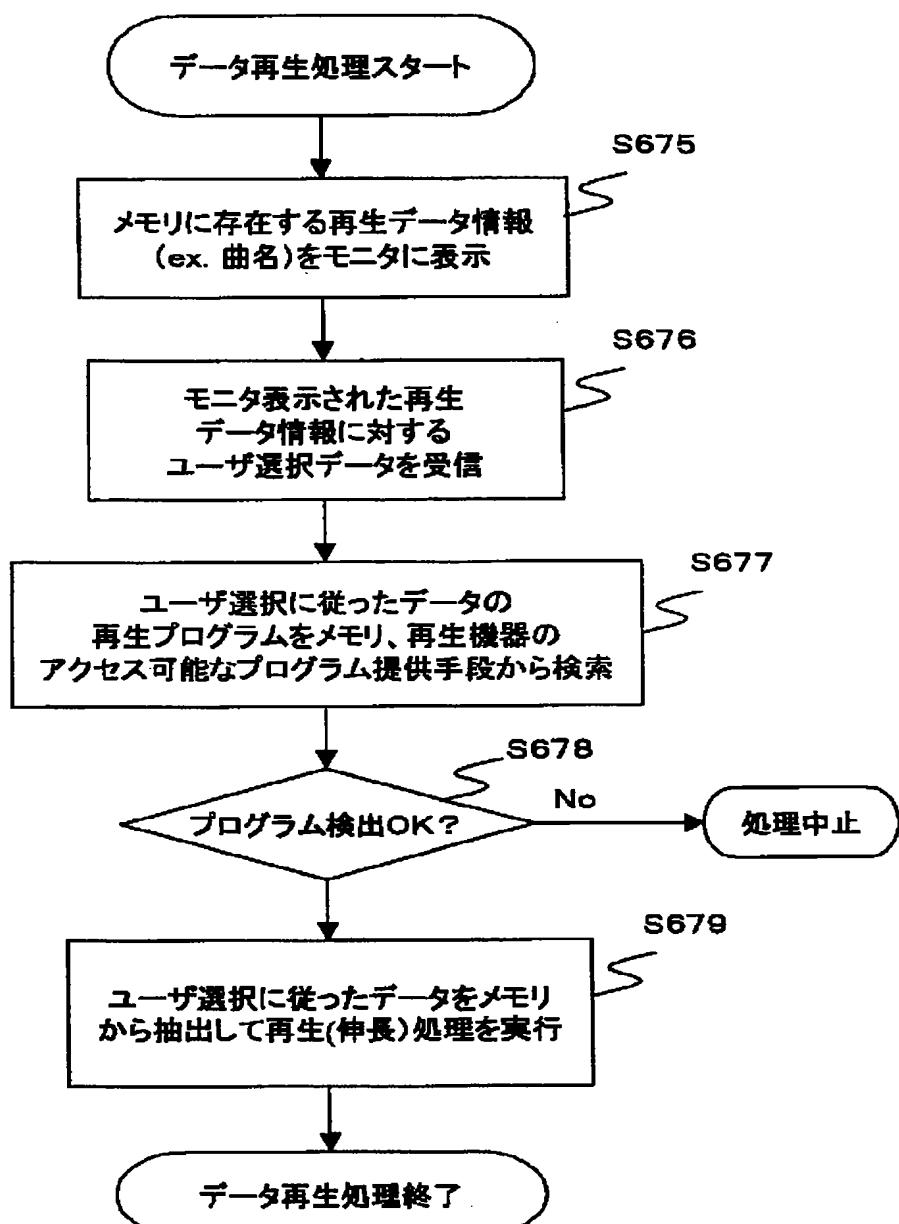
【図60】



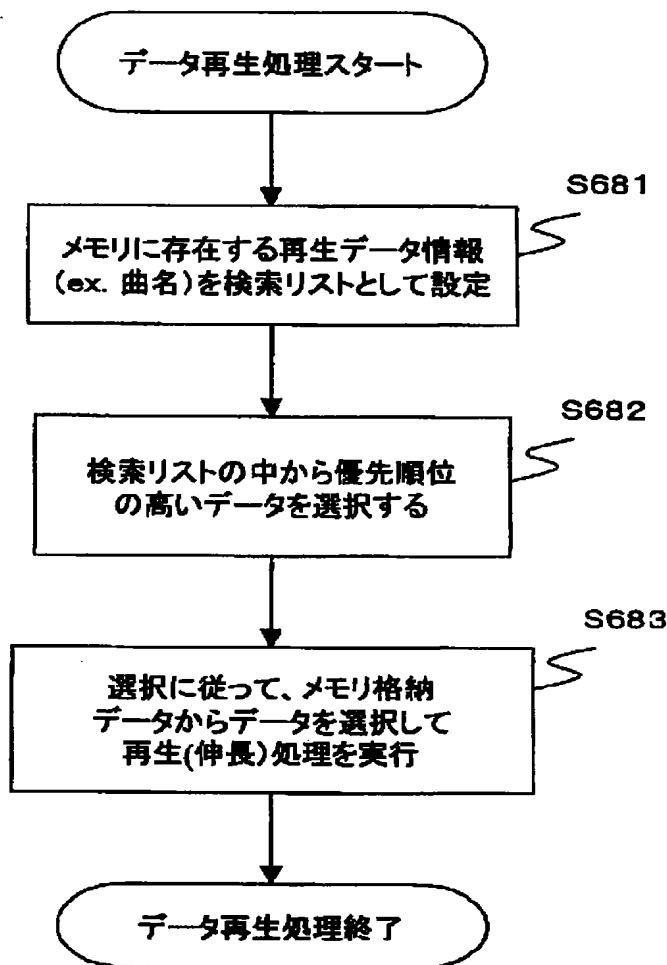
【図62】



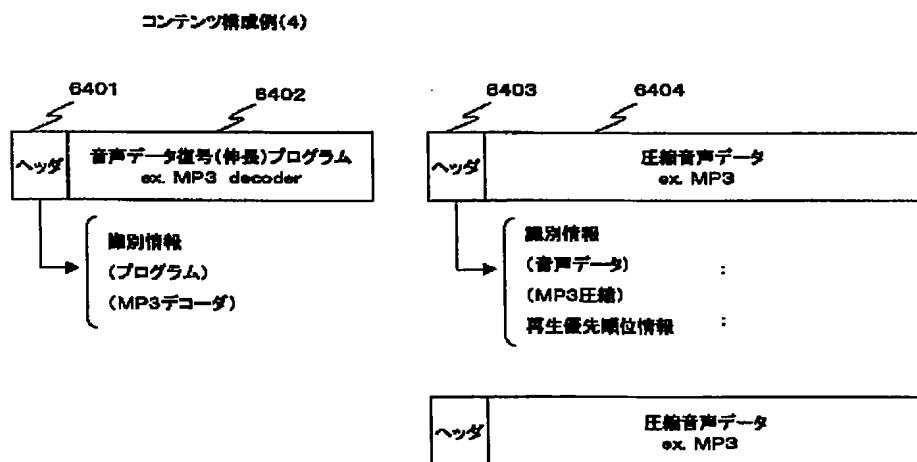
【図64】



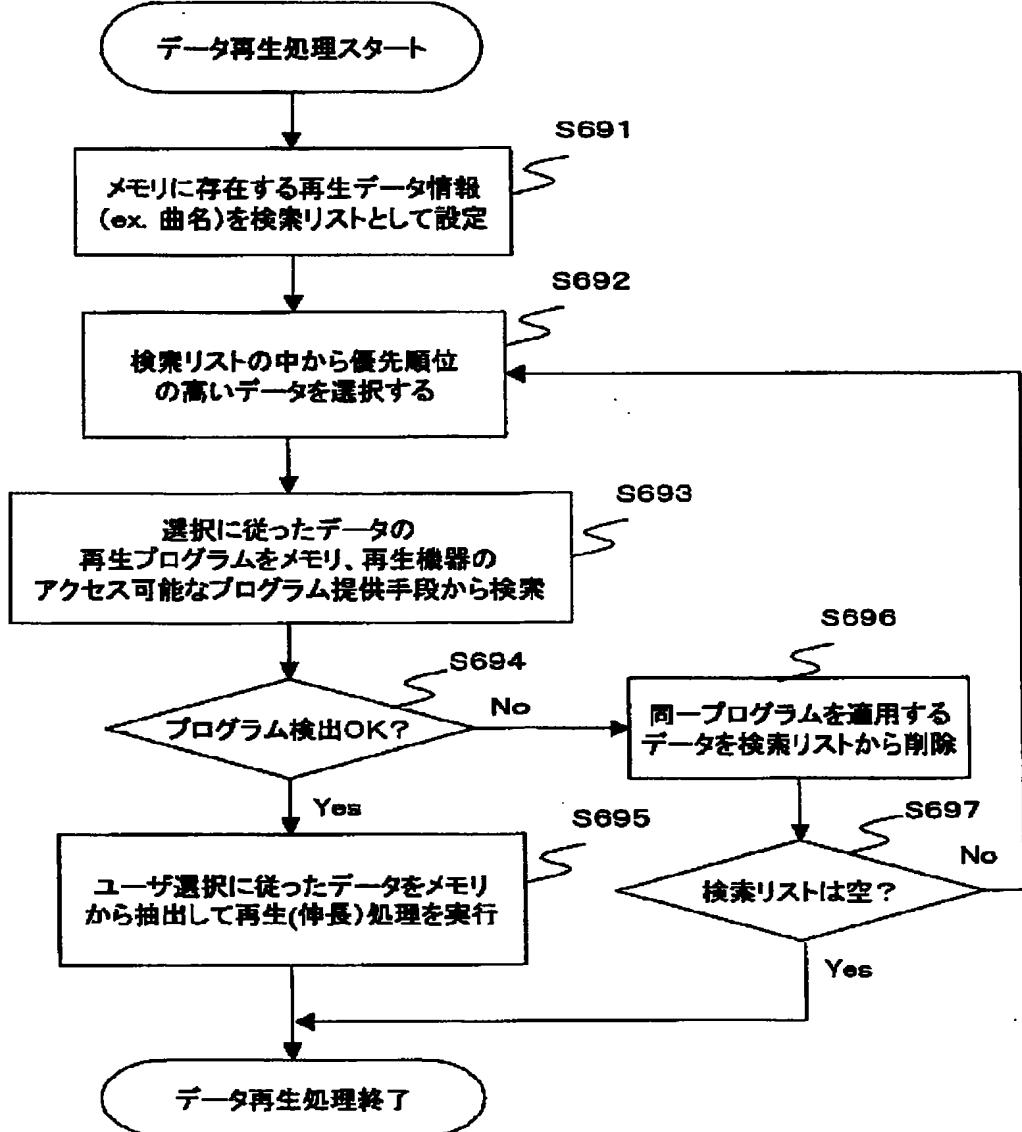
【図66】



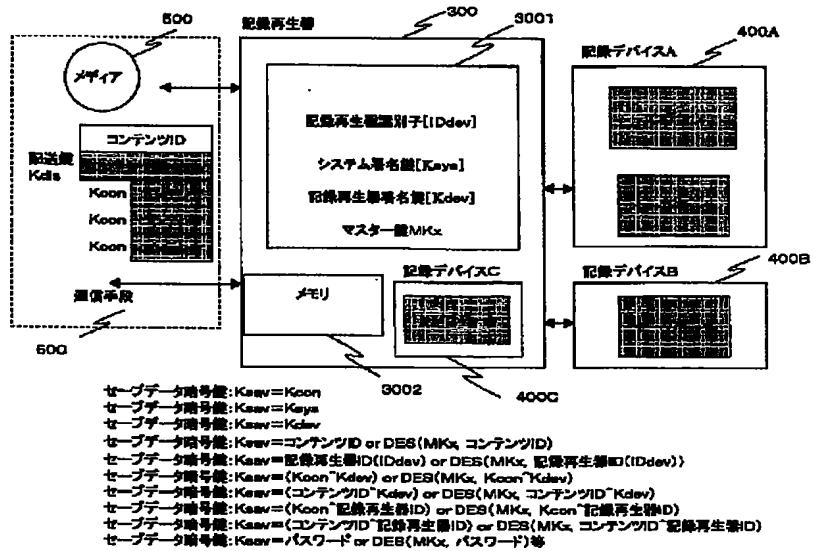
【図67】



【図68】



【図 6 9】



【図 7 6】

データ管理ファイル(2)

データ番号	コンテンツ識別子 (ゲームID)	記録再生器識別子 (IDdev)	記録再生器制限
1	12345678...	56789012...	しない
2	ABCDEF12...	09876543...	する
3	122457678...	58834762...	する
:	:	:	:

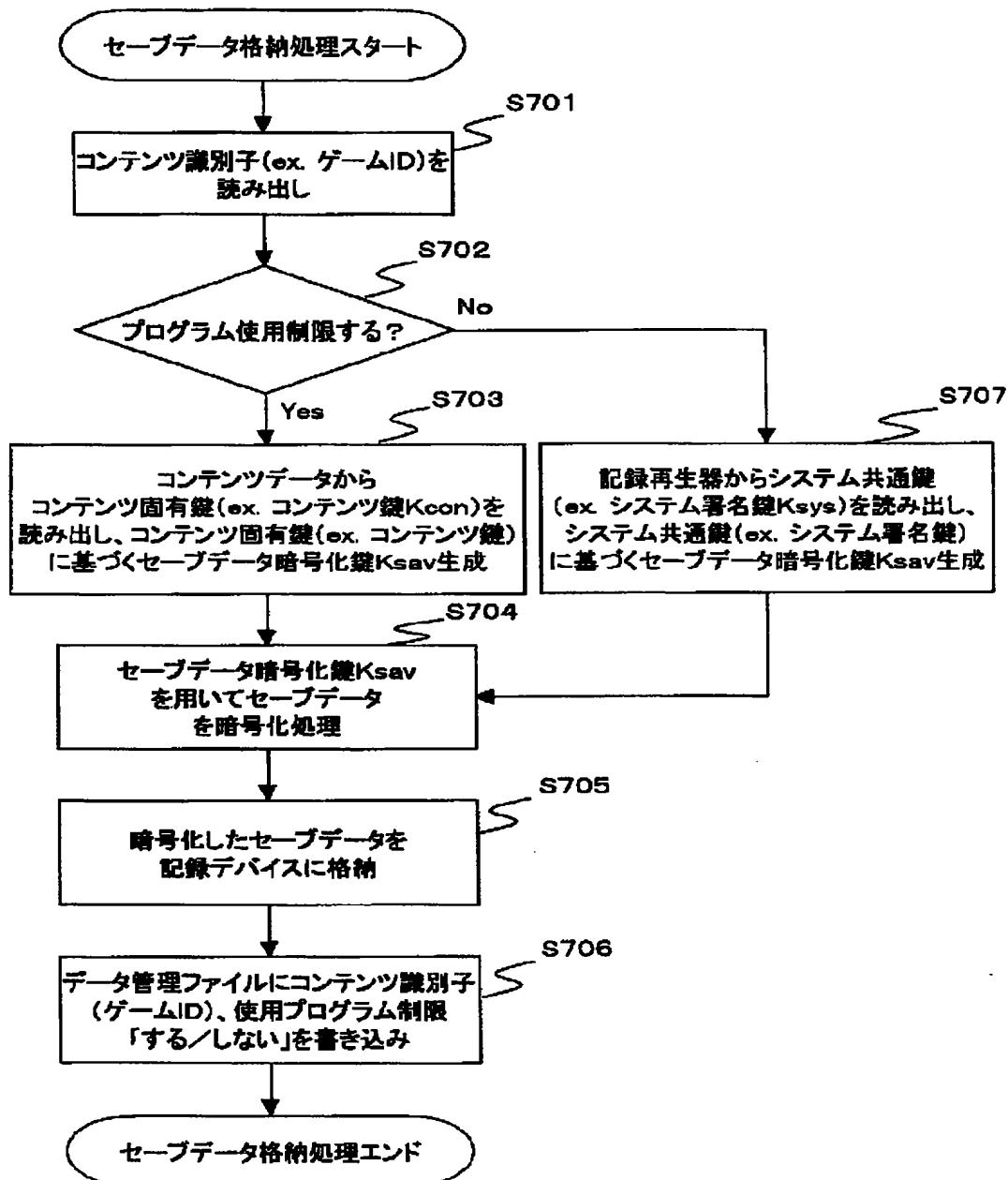
【図 8 1】

データ管理ファイル(3)

データ番号	コンテンツ識別子 (ゲームID)	記録再生器識別子 (IDdev)	プログラム使用制限	記録再生器制限
1	12345678...	56789012...	する	しない
2	ABCDEF12...	09876543...	する	する
3	122457678...	58834762...	しない	する
:	:	:	:	:

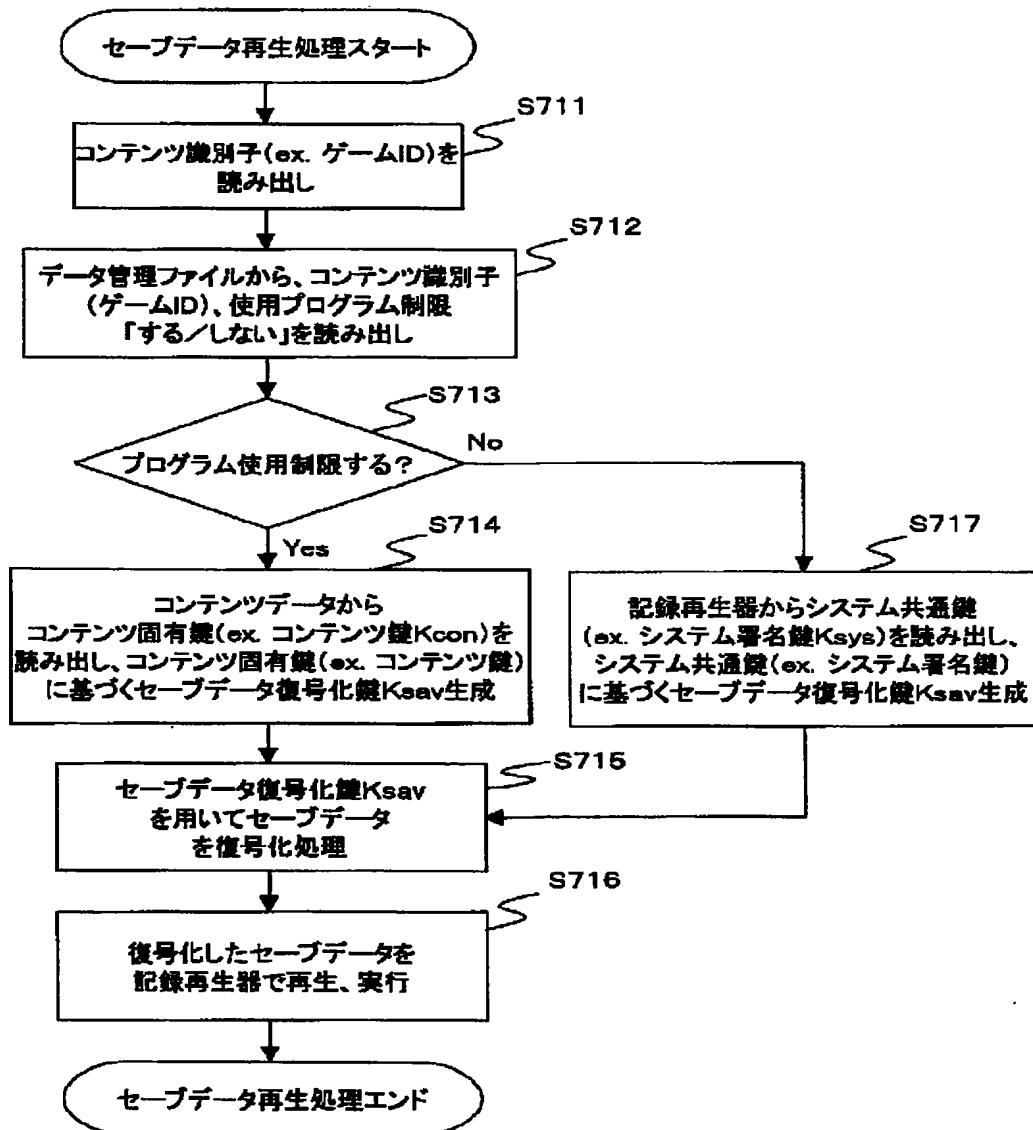
【図70】

(1)コンテンツ固有鍵、orシステム共通鍵を使用したセーブデータ格納処理例



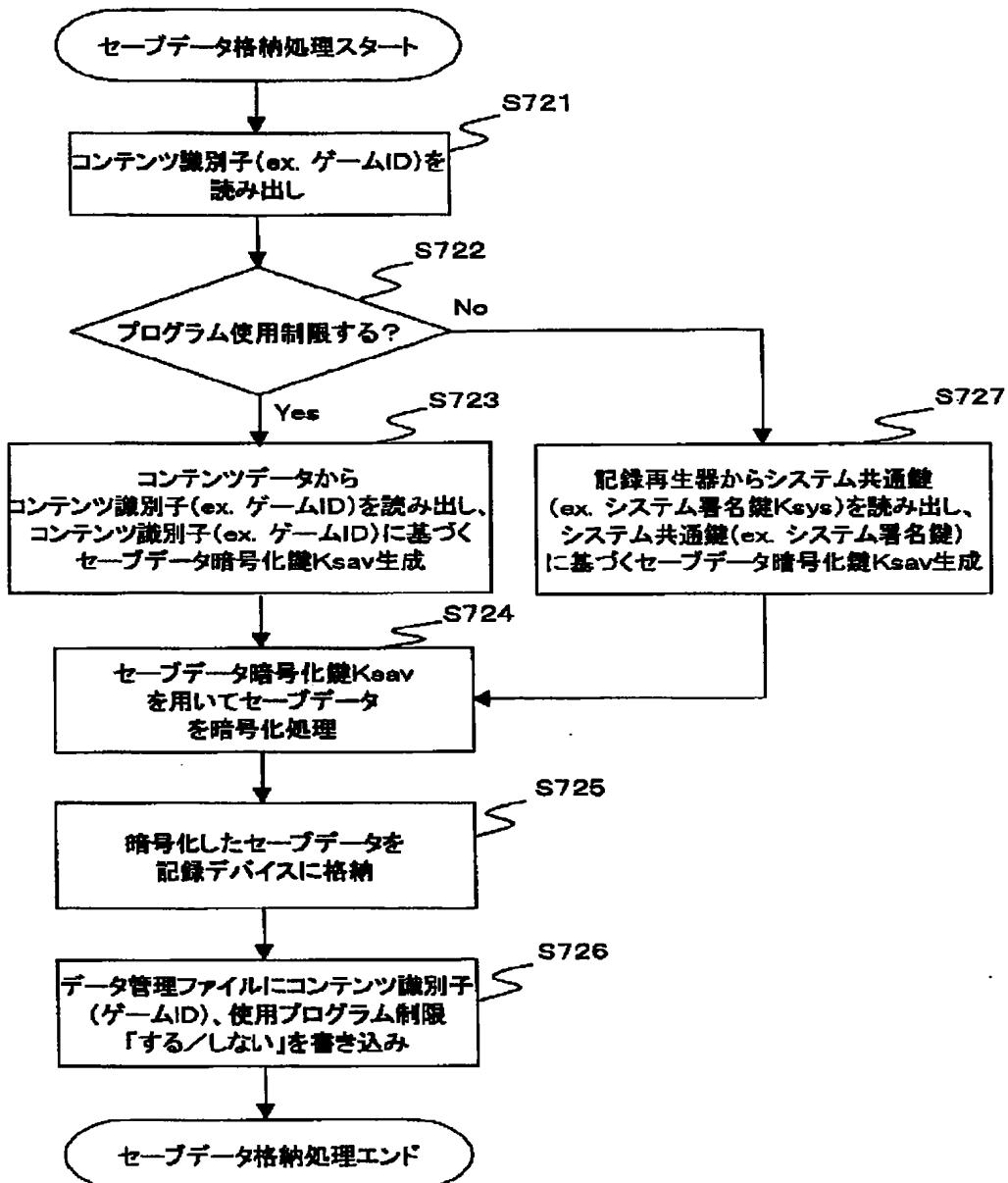
【図72】

(2)コンテンツ固有鍵、orシステム共通鍵を使用したセーブデータ再生処理例



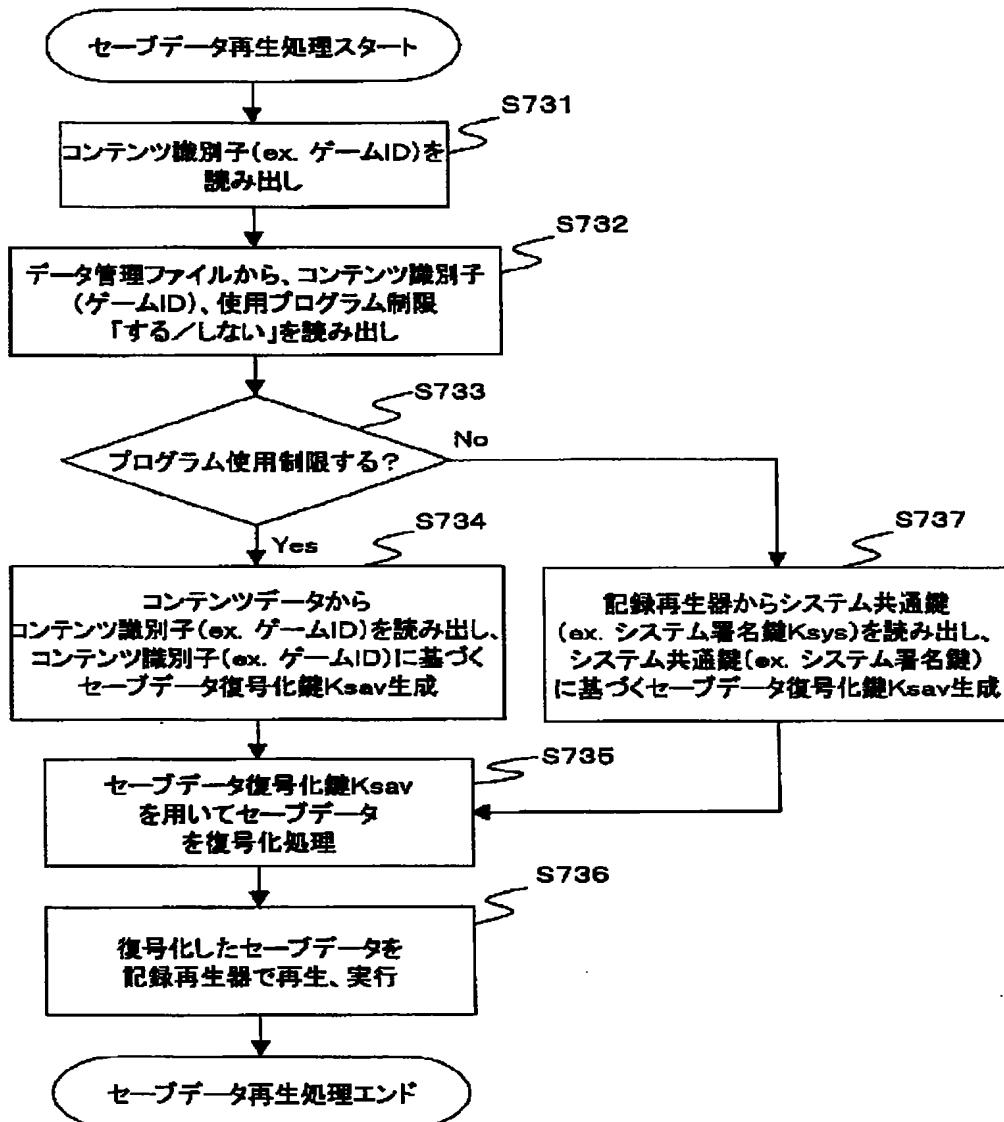
【図73】

(3)コンテンツID、orシステム共通鍵を使用したセーブデータ格納処理例



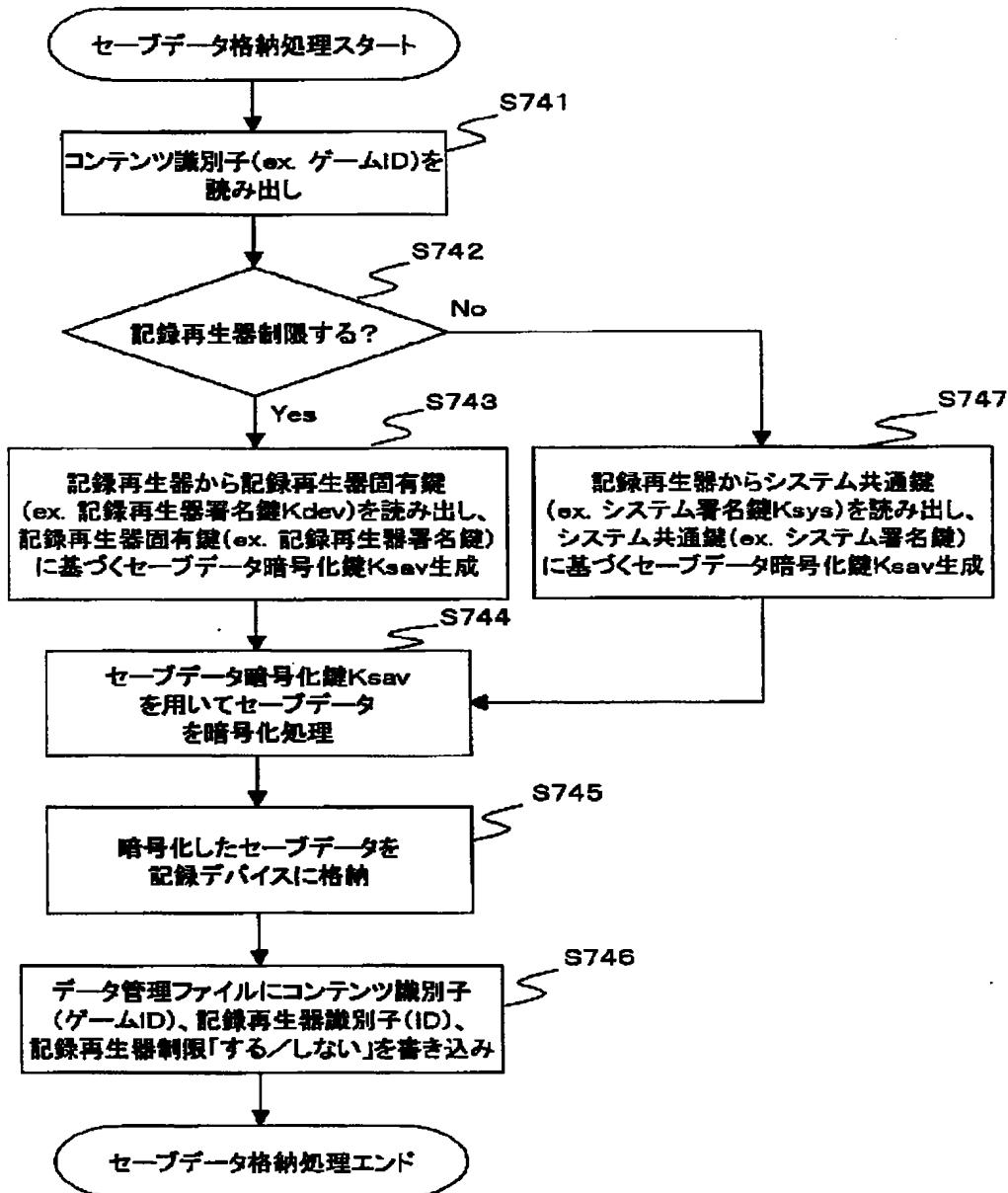
【図74】

(4)コンテンツID、oシステム共通鍵を使用したセーブデータ再生処理例



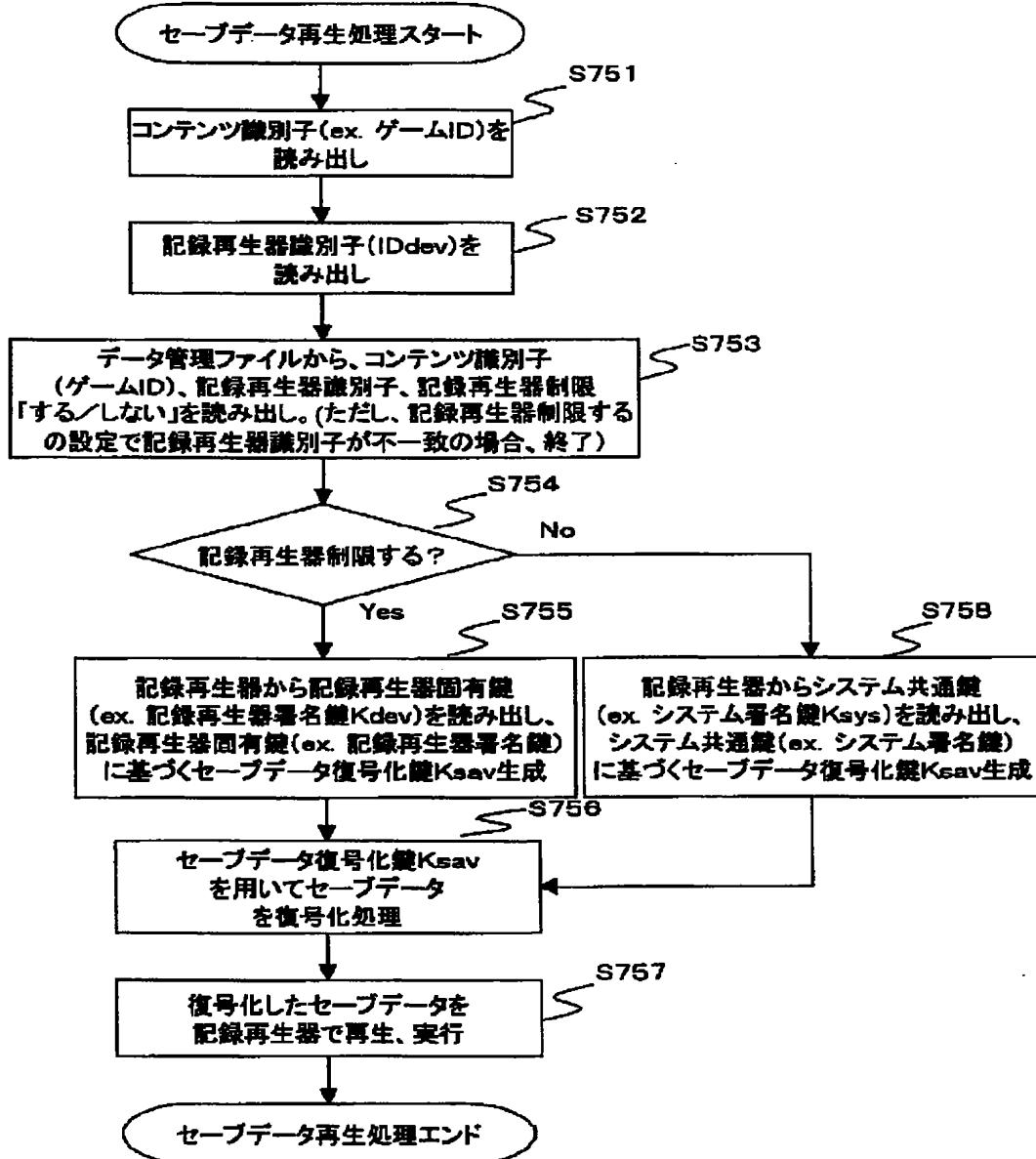
【図75】

(5)記録再生器固有鍵、or システム共通鍵を使用したセーブデータ格納処理例



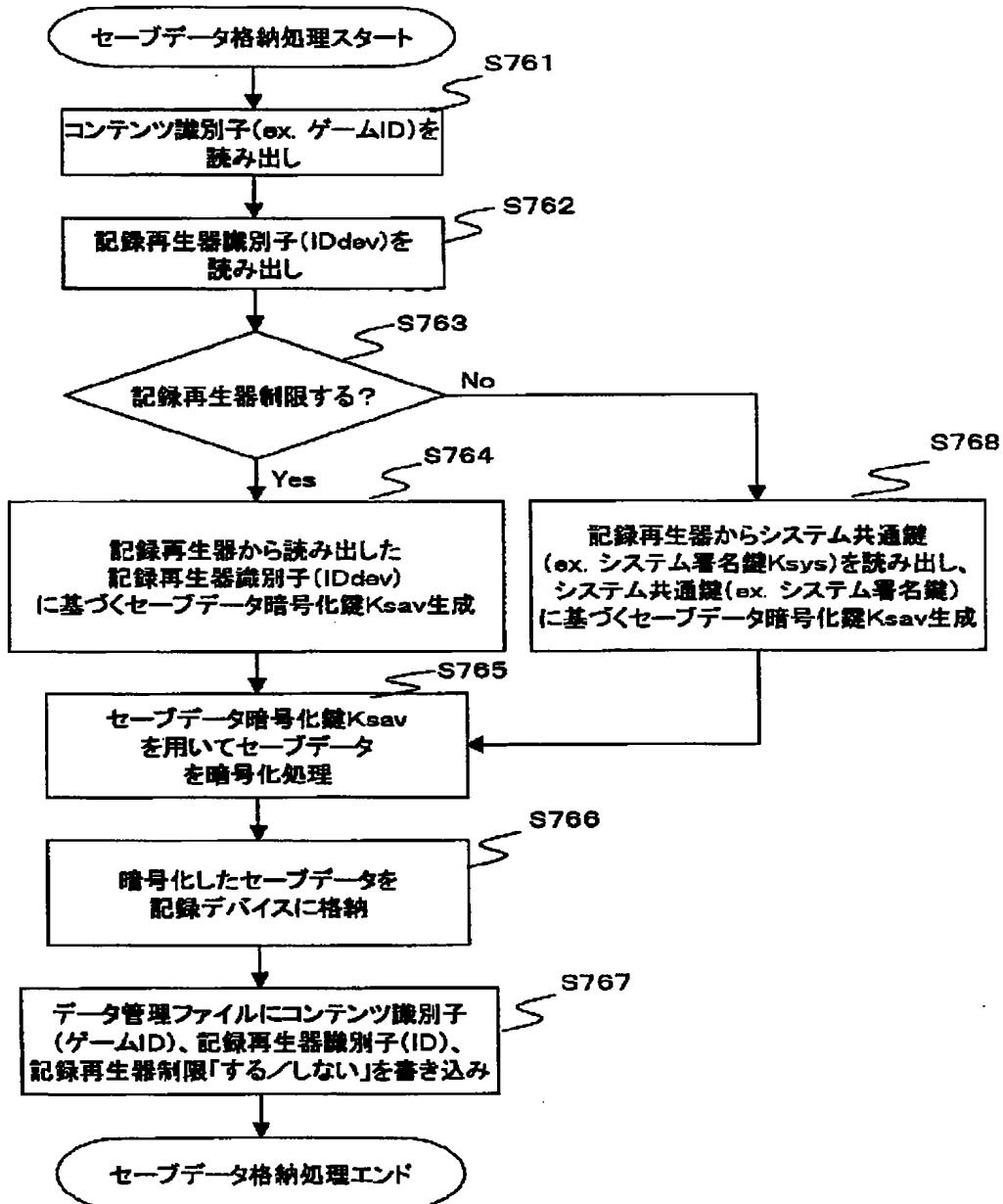
【図77】

(6)記録再生器固有鍵、or システム共通鍵を使用したセーブデータ再生処理例



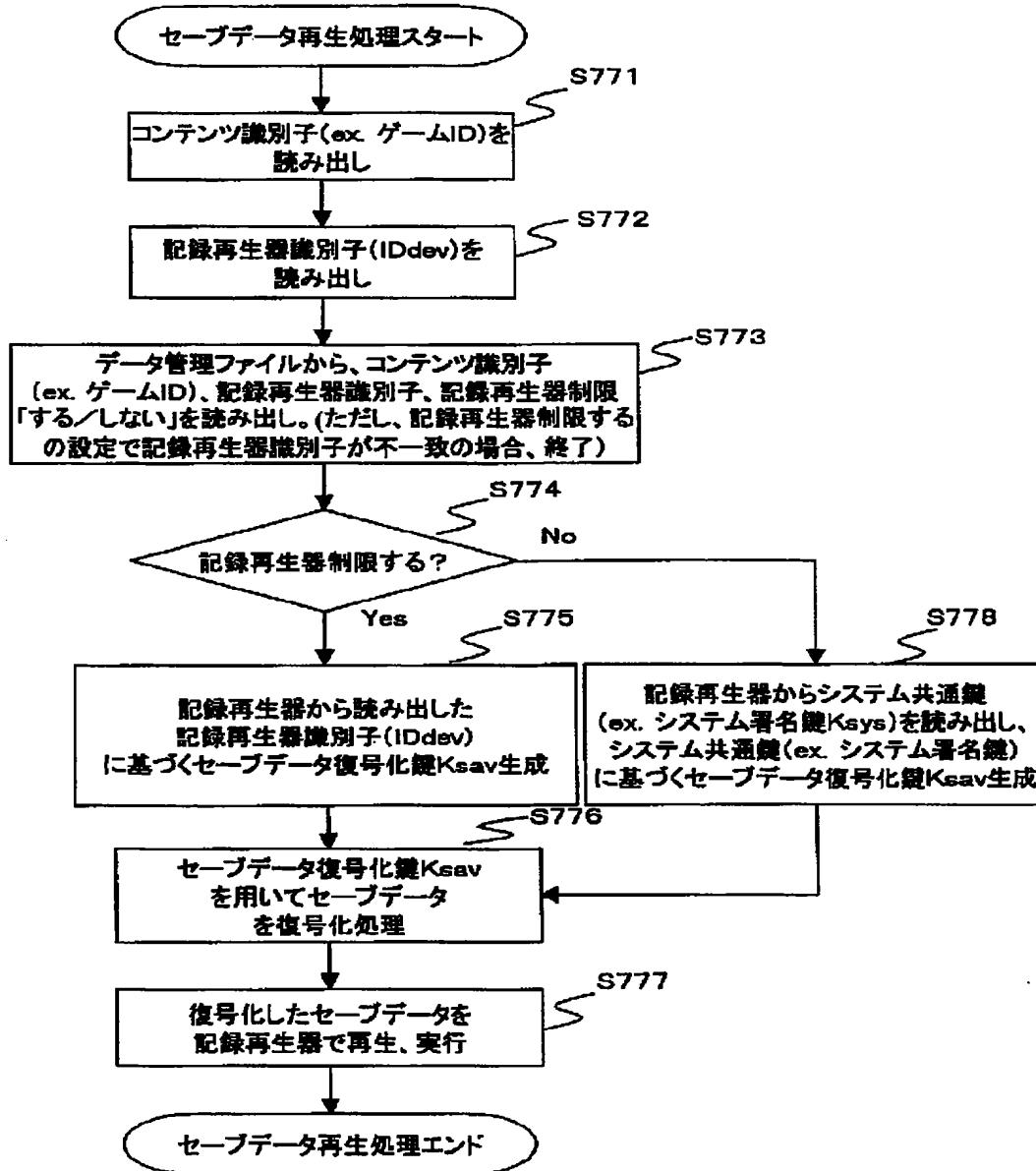
【図78】

(7)記録再生器識別子、or システム共通鍵を使用したセーブデータ格納処理例



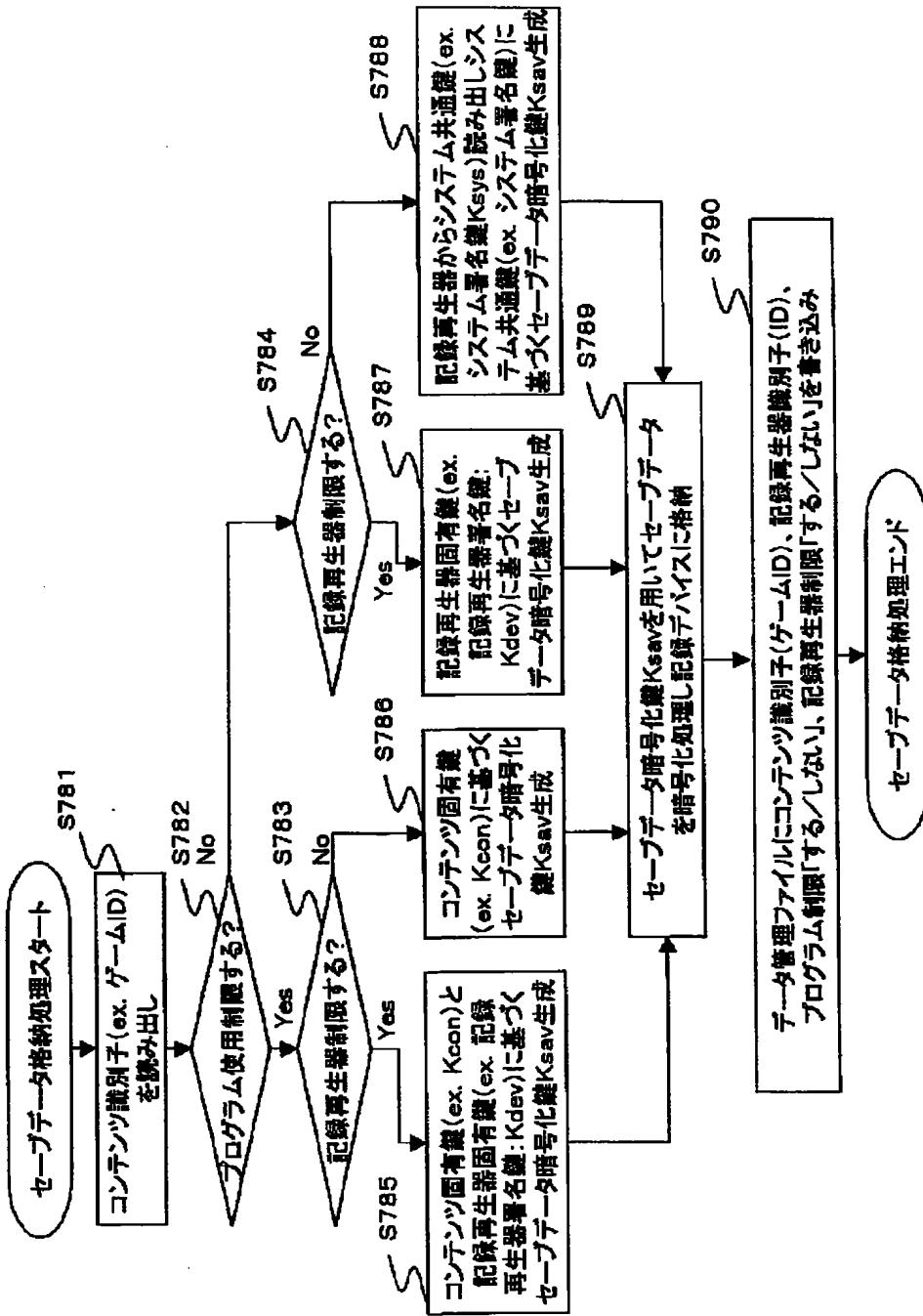
【図79】

(8)記録再生器識別子、or システム共通鍵を使用したセーブデータ再生処理例

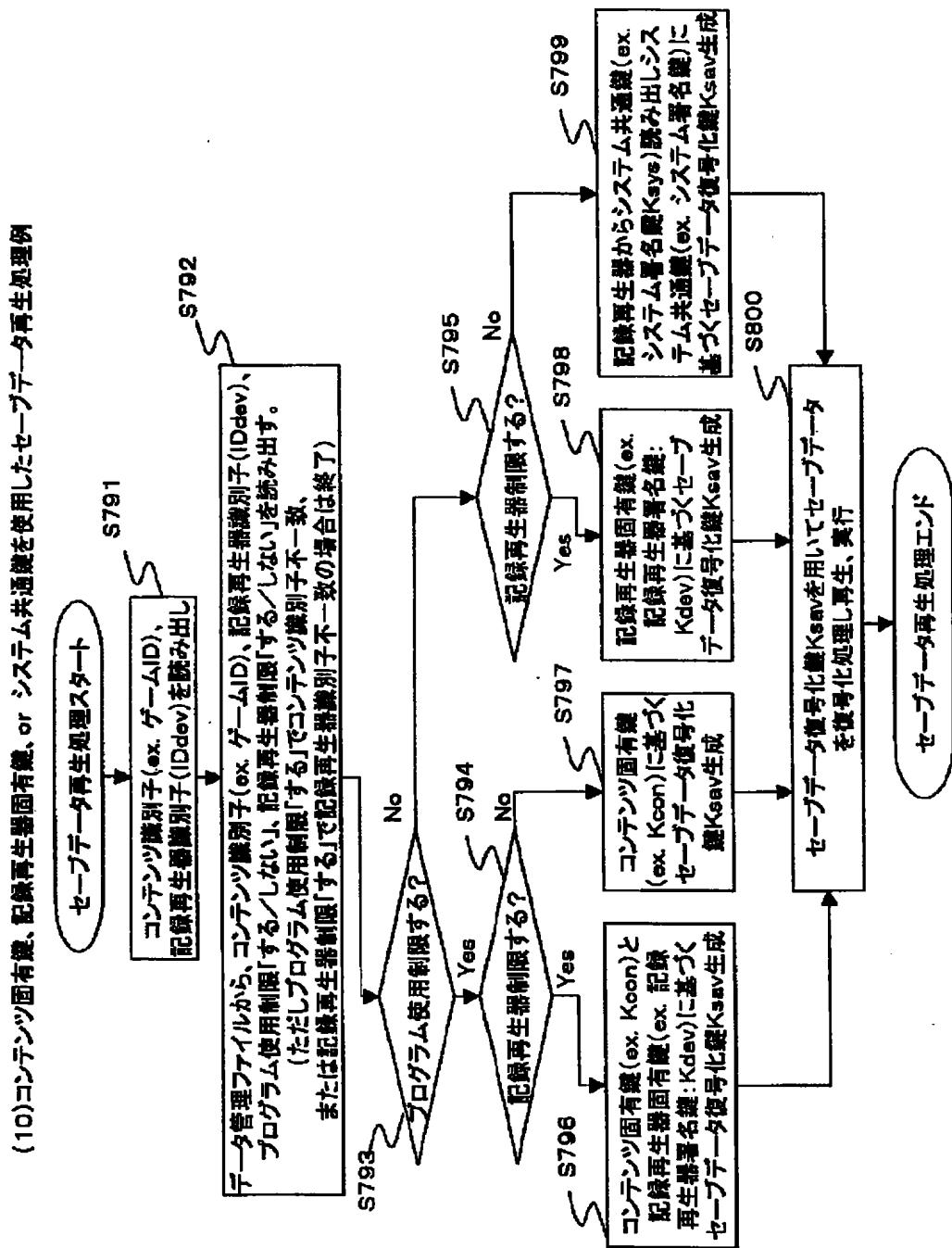


【図80】

(9) コンテンツ固有鍵、記録再生器固有鍵、or システム共通鍵を使用したセーブデータ格納処理例

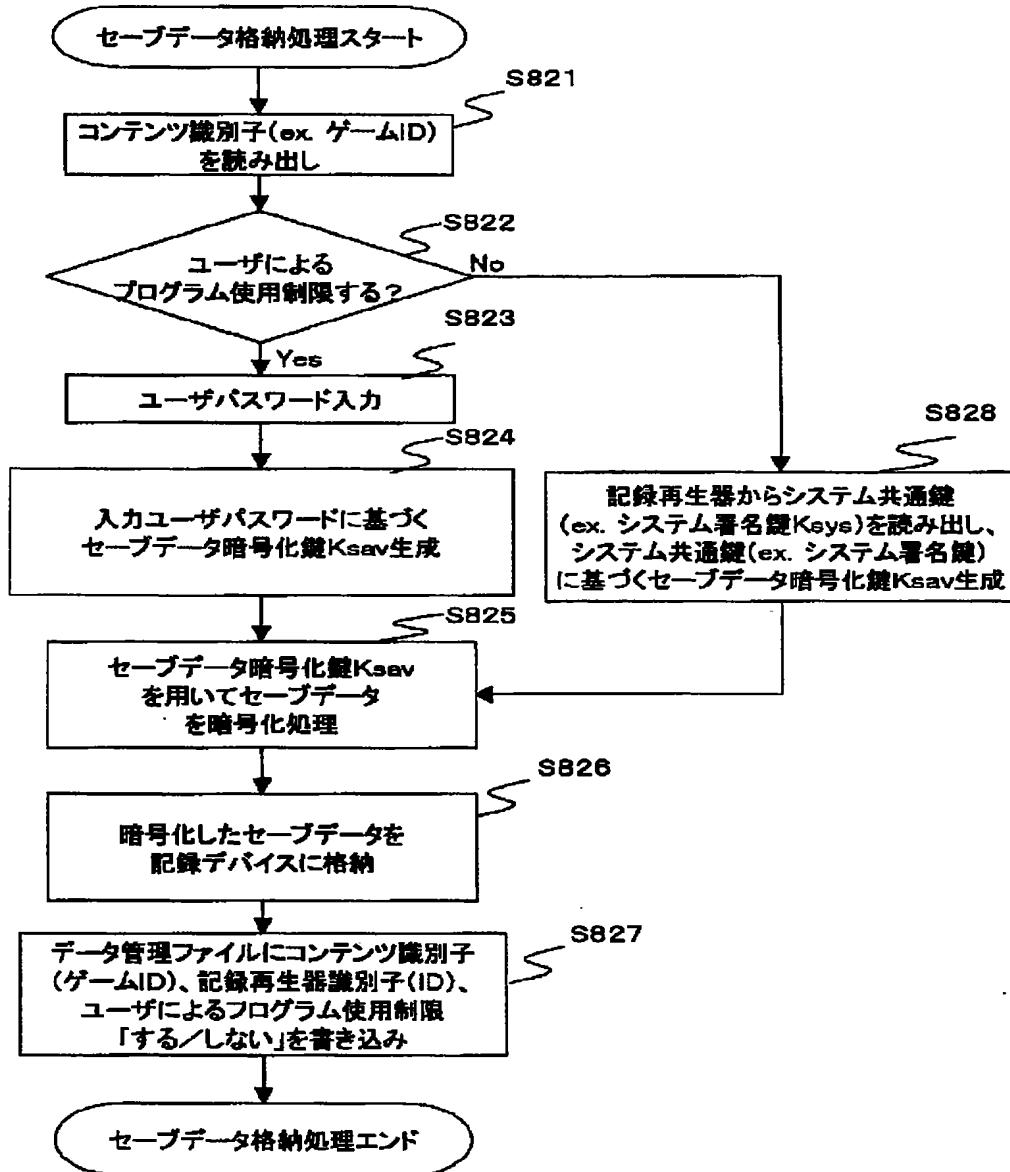


【図82】



【図83】

(11)ユーザパスワード、or システム共通鍵を使用したセーブデータ格納処理例

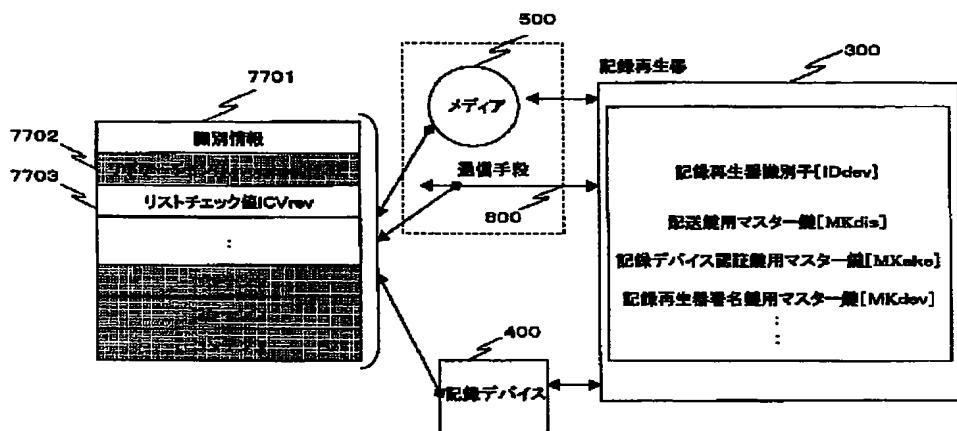


【図84】

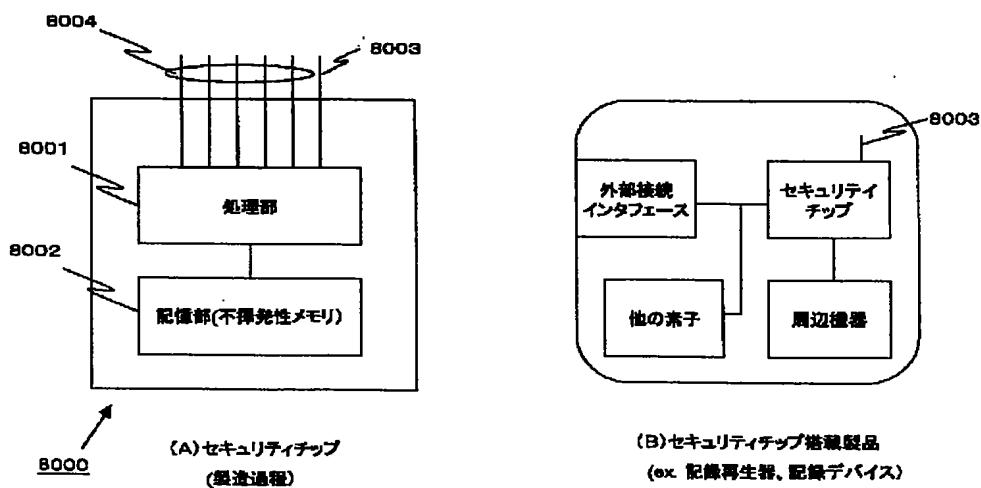
データ管理ファイル(4)

データ番号	コンテンツ識別子 (ゲームID)	記録再生器識別子 (IDdev)	ユーザーによる プログラム使用制限
1	12345678...	56789012...	する
2	ABCDEF12...	09876543...	する
3	122457678...	58834762...	しない
:	:	:	:

【図86】

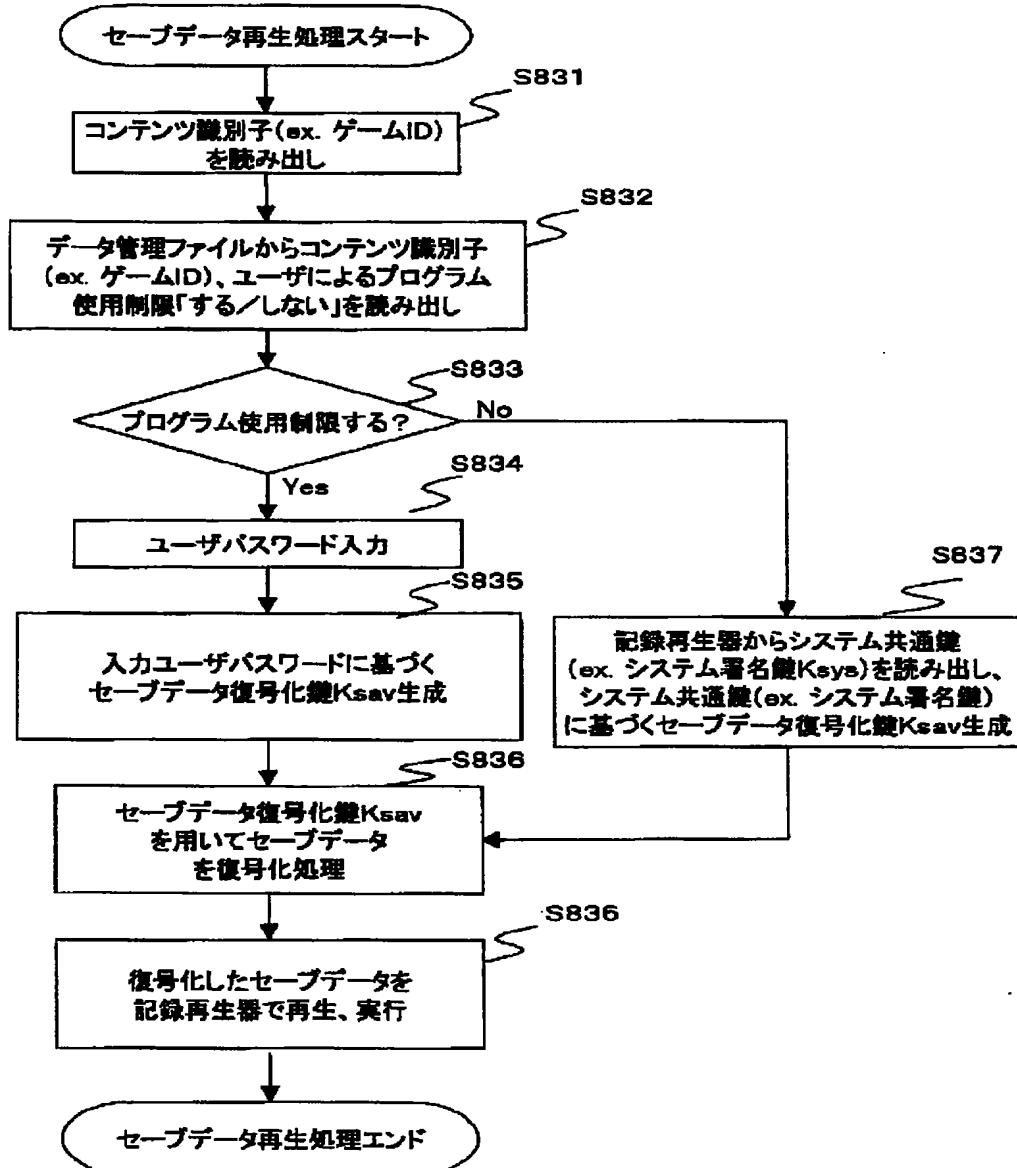


【図89】

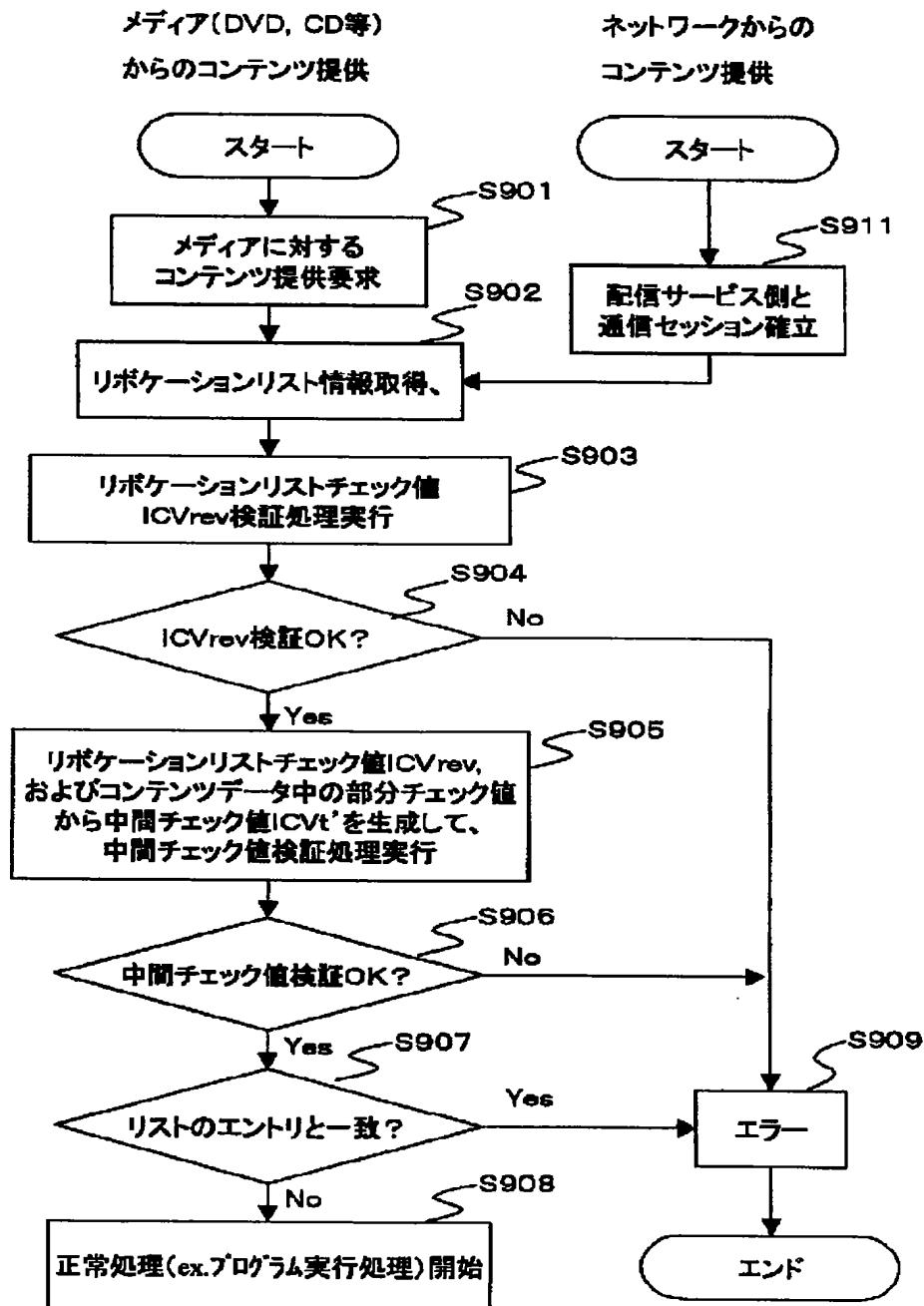


【図85】

(12)ユーザパスワード、or システム共通鍵を使用したセーブデータ再生処理例

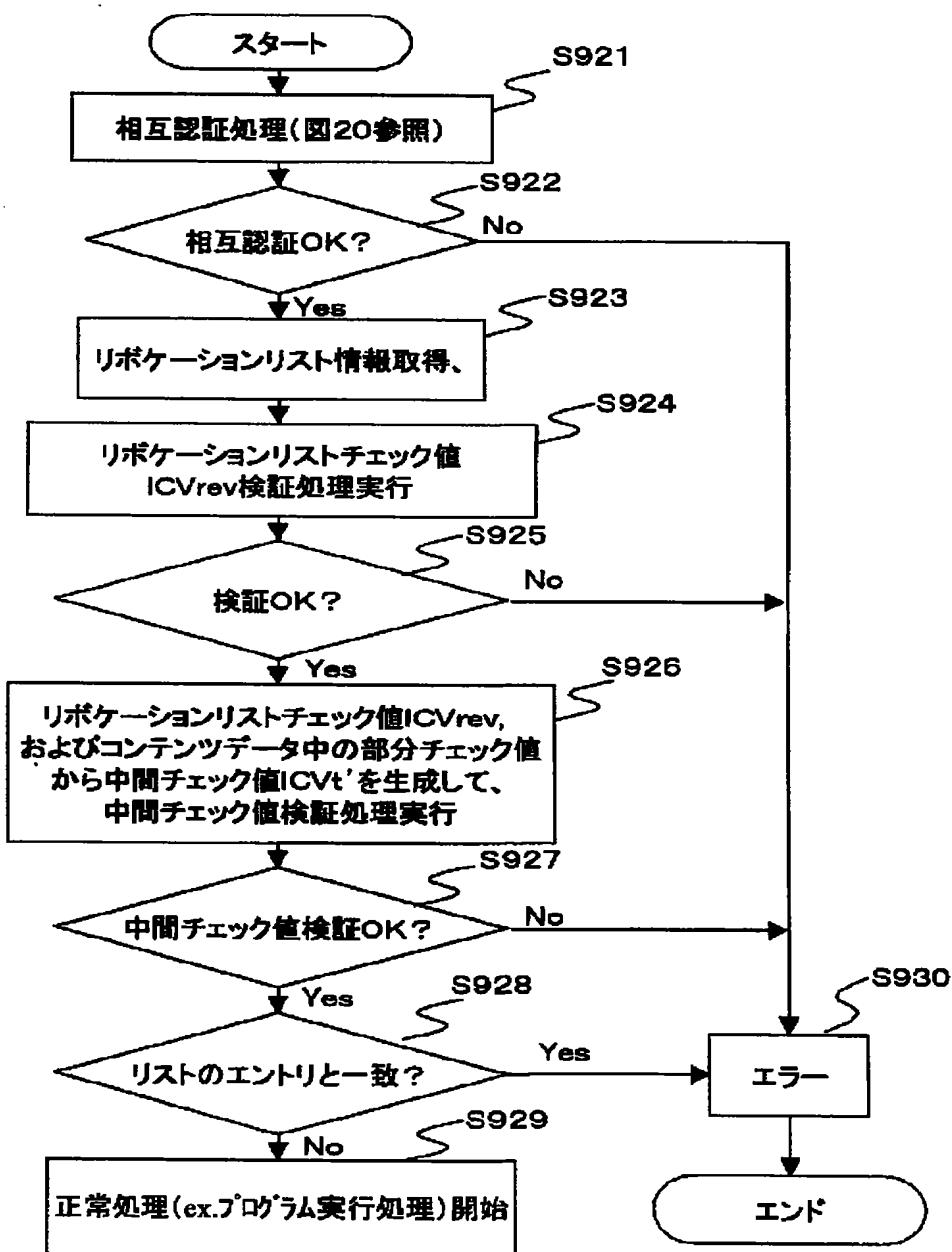


【図87】



【図88】

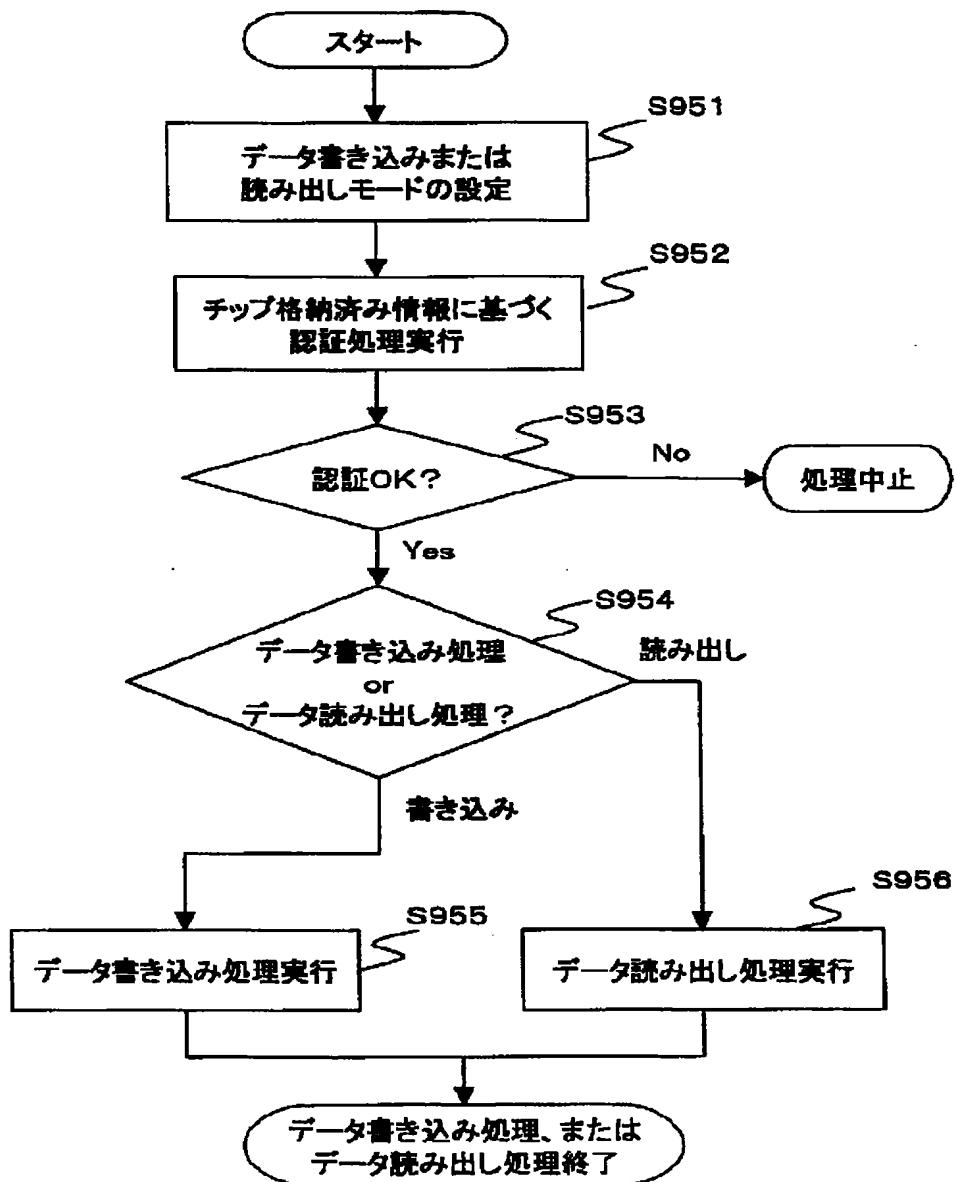
記録デバイス(メモリカード等)からのコンテンツ提供



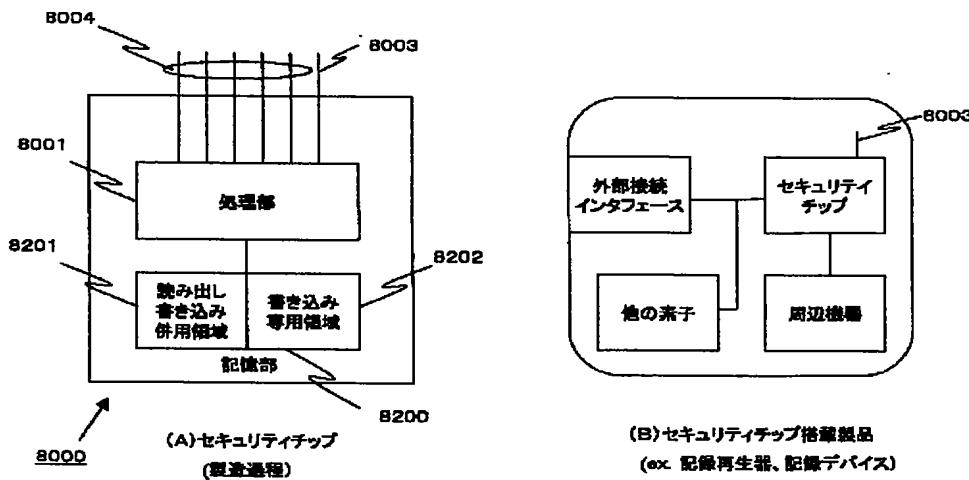
【図90】

セキュリティチップ

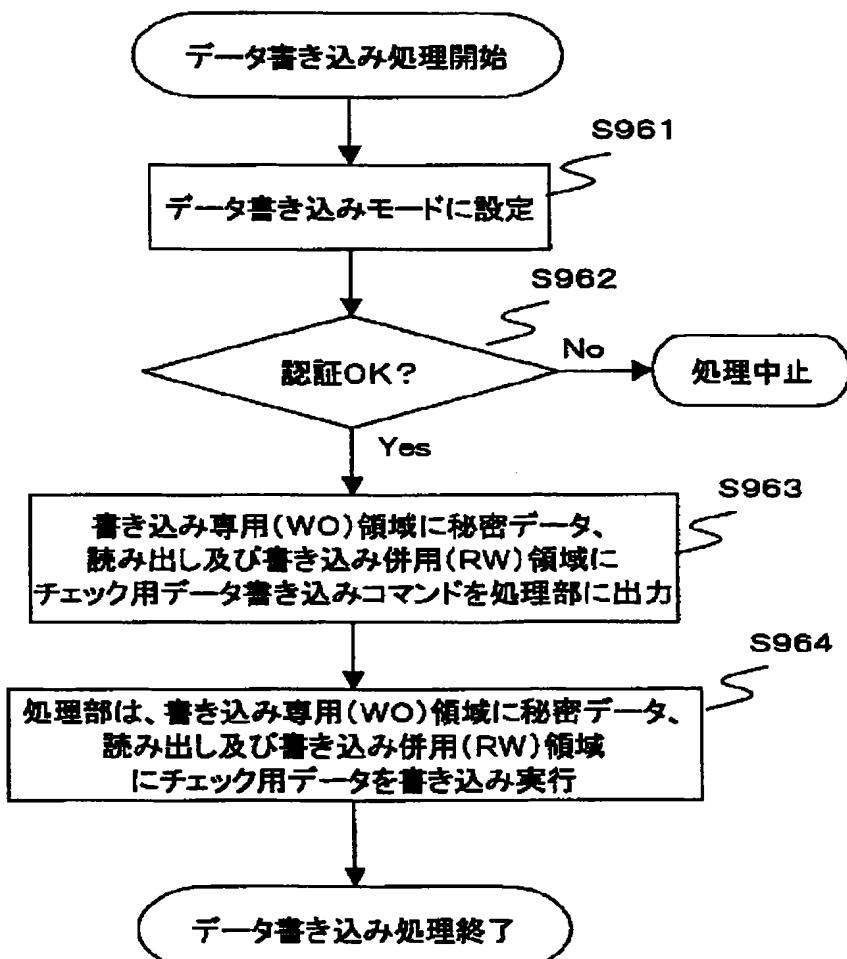
製造処理フロー



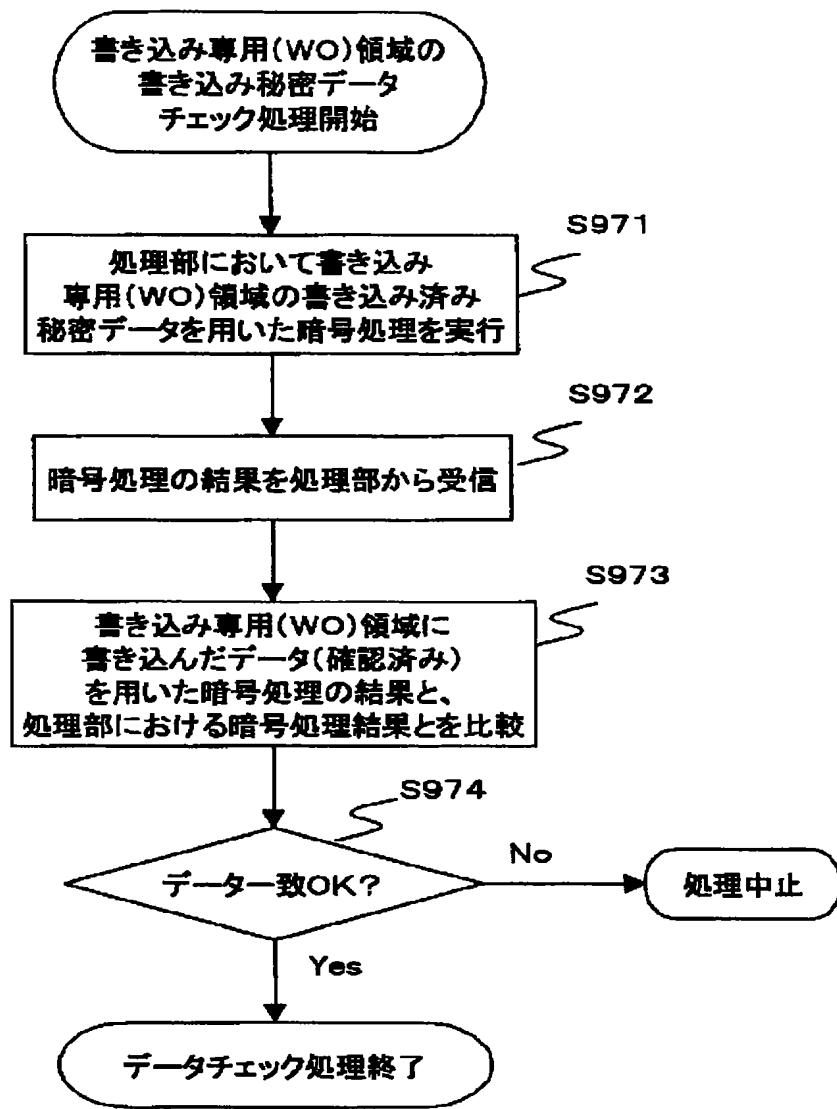
【図91】



【図92】



【図93】



フロント

(129)

特開平13-209583

F ターム(参考) 5B017 AA03 BA07 BB09 CA15 CA16

5B082 EA12

5D044 AB01 AB05 AB07 BC01 I